WEST VIRGINIA HEALTH CARE AUTHORITY

STATE PRIVACY OFFICE

2016 PRIVACY REQUIREMENTS

TABLE of CONTENTS

Page

Privacy Requirements 4

Scope 4

1.0. Federal 5

1.1. Privacy Act of 1974, Section 7 5

1.2. Tax Reform Act of 1976 7

1.3. Omnibus Reconciliation Act of 1990, § 2201(c) 10

1.3.1. Federal Tax Return Information 11

1.4. Health Insurance Portability and Accountability Act of 1996, ("HIPAA") 14

1.4.1 HIPAA "Privacy Rule" 16

1.4.2. HIPAA "Security Rule" 21

1.4.3. HIPAA Breach Notification Rule 25

1.5. The Affordable Care Act; Affordable Insurance Exchanges 30

1.6. Federal Trade Commission's Health Breach Notification Rule 32

1.6.1. FTC Enforcement of PII and PHI Data Security of HIPAA Covered Entities and Business Associates 36

1.7. Confidentiality of Substance Abuse Records, Reports of Violations 41

1.8. Gramm-Leach Bliley-Act (GLB) 43

1.8.1. Gramm-Leach-Bliley Act (GLB), "Safeguards Rule" 47

1.9. Fair Credit Reporting Act as amended (FCRA) (including the Fair and Accurate Credit Transactions Act of 2003 (FACT Act)) 50

1.9.1. Identity Theft "Red Flags" Rule 54

1.10. Family Educational Rights and Privacy Act of 1974 (FERPA) 58

1.11. Driver's Privacy Protection Act 61

1.12. Telephone Consumer Protection Act, Telemarketing Sales Rules 63

1.13. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, (CAN-SPAM Act) 66

1.14. Junk Fax Prevention Act of 2005 68

1.15. Children's On-line Privacy Protection Act (COPPA) 70
1.16. Cable Communications Policy Act (CCPA) 73
1.17. Video Privacy Protection Act 75
1.18. United States Patriot Act 77
1.19. Computer Fraud and Abuse Act of 1986 (CFAA) 79
1.20. National Crime Prevention and Privacy Compact (NCPPC) 82
1.21. Genetic Information Nondiscrimination Act of 2008 (GINA) 83
1.22. Real ID Act of 2005 87
1.23. Electronic Communications Privacy Act of 1986 89
1.24. Federal Aviation Administration 92
2.0. Federal Case Law 94
A. Freedom of Information Act (FOIA) 94
B. Privacy 95
C. Driver's Privacy Protection Act of 1994 110
D. Fair Credit Reporting Act 111
3.0 West Virginia 113
3.1. Executive Order No. 6-06 (August 16, 2006) 113
3.2. Freedom of Information Act 115
3.3. Records Management and Preservation of Essential Records Act 117
3.4. Information Services and Communications Division 119
3.5. The Uniform Electronic Transactions Act 120
3.6. State Health Privacy Laws 122
3.7. West Virginia Health Information Network 123
3.8. Maxwell Governmental Access to Financial Records Act 125
3.9. Confidentiality and Disclosure of Tax Returns and Return Information 126
3.10. Uniform Motor Vehicle Records Disclosure Act 131
3.11. Consumer Credit and Protection Act, General Consumer Protection 133
3.12. Computer Crime and Abuse Act 134
3.13. Bureau for Child Support Enforcement, Confidentiality 135
3.14. Sharing of Domestic Violence Information 136
3.15. The Emergency Medical Services Act 137

3.16. Insurance Commissioner Rule, "Privacy of Consumer Financial and Health Information" 138

3.16.1. External Review of Issuers' Adverse Health Insurance Determinations 139

3.17. All-Payer Claims Database 140

3.18. Breach of Security of Consumer Information Act 141

3.19. Governmental Ethics Act 143

3.20. Ratification of the National Crime Prevention and Privacy Compact (NCPPC) 144

3.21. Chief Technology Officer Duties Relating To Security of Government Information 145

3.22. State Board of Education: Student Data Accessibility, Transparency, and Accountability Act 146

3.23. Confidentiality of Child and Juvenile Records; Sharing Juvenile Records with Other States; West Virginia Child Welfare Act 148

3.24. Monitoring Inmates Telephone Calls and Mail 150

3.25. Drug Testing for Public Improvements 152

3.26. Verifying Legal Employment Status of Workers 153

3.27. Address Confidentiality Program 155

3.28. Security of Capital Complex, Other State Facilities, and Sensitive or Critical Information 156

4.0. Agency Agreements with Privacy or Security Provisions 158

4.1. Vendor Agreement Clauses 160

5.0. West Virginia Case Law 162

A. State Freedom of Information Act Cases 162

B. Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). 174

C. Federal Telephone Consumer Protection Act (TCPA) 179

6.0. Payment Card Industry Data Security Standards (PCI DSS) 181

Privacy Requirements

Scope

Each Department must continue to operate within its legal authority and restrictions with regard to the collection, use, disclosure, and retention of personally identifiable information (PII). Where the statutes governing PII are more restrictive, they will control. However, if there is no agency, program, or subject matter specific law governing the PII, the more general law will apply.

This report is intended to review laws that impact the Enterprise. Necessarily, there will be privacy laws not covered in this report, as they impact isolated agencies. If a privacy law is not covered in the report, but may have a wide impact, a request should be made to the Executive Branch Privacy Office for inclusion in the next report. This report will be reviewed and updated on an annual basis, with issuance in the fall of each year.

Laws are divided into two categories – Federal and State. Each law is identified by common name, legal citation with a description, implications, and electronic source. Each law is mapped to applicable Privacy Principles.

1.0. Federal

1.1. Privacy Act of 1974, Section 7

5 U.S.C. § 552a (note)

Description:

Except in certain situations, federal, state, and local government cannot deny an individual "any right, benefit, or privilege provided by law because of such individual's refusal to disclose his Social Security account number." This prohibition does not apply in two scenarios. The first is where a federal law mandates disclosure of the SSN. The second is where a federal, state, or local agency "maintain[s] a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual."

Where government requests an individual to disclose his or her SSN, the Department must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it."

While enforcement is not specifically delineated in the law, private individuals have successfully sued state and local government in the 4th Circuit, and other circuits, under this law.

The "Overview of the Privacy Act of 1974," prepared by the Office of Privacy and Civil Liberties (OPCL), United States Department of Justice, discusses the Privacy Act's disclosure prohibition, its access and amendment provisions, and its requirements for agency recordkeeping. This Overview provides reference to, and legal analysis of, court decisions interpreting the Act's provisions and includes policy guidance issued by the Office of Management and Budget pursuant to 5 U.S.C. § 552a(v). The 2015 edition of the Overview was issued in July 2015, and has been updated to include cases through May, 2014.

Implications:

- Departments must assess where they collect the SSN and tie it to a right, benefit, or privilege where they are mandated by federal law to do so and where they have a system of records, required by statute or regulation, in existence before January 1, 1975.
- Where Departments cannot collect the SSN under the Privacy Act, they must assess their business operations and implement an alternative method of identifying individuals.
- Where Departments can continue to collect the SSN under the Privacy Act, they must provide notice consistent with this law.
- Where Departments collect the SSN lawfully, they must not use it for any secondary purpose that does not meet the Privacy Act requirements and is not delineated in the Notice.

- Departments must adopt policies and procedures regarding SSN collection, SSN use, and display of the Privacy Act notice.

Source:

5 U.S.C. § 552a – Records maintained on individuals
http://www.law.cornell.edu/uscode/text/5/552a (See note on "Disclosure of Social Security Number")

CRS Report RL 30318 – The Social Security Number, (February, 8, 2012)
http://greenbook.waysandmeans.house.gov/sites/greenbook.waysandmeans.house.gov/files/2012/documents/RL30318_gb.pdf

U. S. Justice Department – Overview of Privacy Act of 1974
- https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition

Social Security Number Usage
http://www.justice.gov/opcl/social-security-number-usage

Principles:

Notice, Minimum Necessary and Limited Use

1.2. Tax Reform Act of 1976

42 U.S.C. § 405(c)(2)

Description:

The Tax Reform Act of 1976 amended the Social Security Act by (1) authorizing states to use the SSN as an identifier in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law, (2) allowing states to require individuals to furnish their SSN to the state with regard to these programs, and (3) codifying the use of the SSN for federal tax purposes.

Since 1976, 42 U.S.C. § 405 has been amended on several occasions. For example, 42 U.S.C. § 405 was amended to provide that the provisions of IRC § 7213(a)(1), (2) and (3) apply to the willful disclosure to any person of social security account records and related records obtained or maintained by the person pursuant to a provision of law enacted after September 30, 1990 in the same manner and to the same extent as such paragraphs apply with respect to the unauthorized disclosure of returns and return information described in IRC § 7213. Additionally, IRC § 7213(a)(4) applies with respect to the willful offer of any item of material value in exchange for any social security account number or related record in the same manner and to the same extent as paragraph (4) applies with respect to offers in exchange for any return or return information described in that paragraph.

The Social Security Number Protection Act of 2010, Public Law 111-318, was enacted to limit access to social security account numbers. Federal, State, and local government agencies are prohibited from displaying the social security account number of any individual, or any derivative of such number, on any check issued for any payment by the Federal, State, or local government agency. Additionally, no Federal, State, or local government agency may employ or enter into a contract for the use or employment of prisoners in any capacity that would allow prisoners' access to the social security account numbers of other individuals.

States and political subdivisions may, however, authorize blood donation facilities to utilize social security account numbers for the purpose of identifying blood donors. Additionally, Social security account numbers may be used to identify duplicate names of individuals on master lists used for jury selection purposes and to identify individuals on such lists who are ineligible to serve on a jury by reason of their conviction for a felony.

The Patient Protection and Affordable Care Act (PPACA), Public Law 111-148, authorizes the United States Secretary of Health and Human Services and Health Insurance Exchanges established pursuant to 42 U.S.C, § 18031 to collect and use the names and social security numbers of individuals. The Medicare Access and CHIP Reauthorization Act of 2015 (MACRA), Pub. L. 114-10 was recently passed by Congress. MACRA prohibits displaying, coding, or embedding Social Security account numbers on Medicare cards issued to an individual who is entitled

to benefits under Medicare Part A or enrolled under Part B and requires that the use of any other identifier on such card is not identifiable as a Social Security account number (or derivative thereof).

Note: Congress has passed additional laws over the years allowing states to use the SSN as an identifier in a variety of programs. *See* Congressional Research Service report below. The Welfare Reform Act of 1996 is one example that amended the Social Security Act requiring States to collect social security numbers for any professional license, driver's license, occupational license, or marriage license.

Implications:

- Use of the SSN as an identifier in certain instances is authorized by federal law.
- As Departments develop their notices and determine from a business process standpoint that they must use the SSN as an identifier, they must identify the federal law which gives them the authority to do so. This law may provide the requisite authority for the SSN collection.

Source:

42 U.S.C. § 405 – Evidence, procedure, and certification for payments
http://www.law.cornell.edu/uscode/text/42/405

42 U.S.C. § 408 – Penalties
http://www.law.cornell.edu/uscode/text/42/408

26 U.S.C. § 6109 – Identifying numbers
http://www.law.cornell.edu/uscode/text/26/6109

26 U.S.C. § 7213 – Unauthorized disclosure of information
http://www.law.cornell.edu/uscode/text/26/7213

26 U.S.C. § 7213A – Unauthorized inspection of returns or return information
http://www.law.cornell.edu/uscode/text/26/7213A

42 U.S.C. § 666(a)(13) – Recording of Social Security Numbers in Certain Family Matters
https://www.law.cornell.edu/uscode/text/42/666

Congressional Research Service Report RL 30318 – The Social Security Number (February, 8, 2012)
http://greenbook.waysandmeans.house.gov/sites/greenbook.waysandmeans.house.gov/files/2012/documents/RL30318_gb.pdf

Principles:
Notice, Minimum Necessary and Limited Use

1.3. Omnibus Reconciliation Act of 1990, § 2201(c)

42 U.S.C. § 405(c)(2)(C)(viii)(I)

Description:

The Omnibus Reconciliation Act of 1990 requires that all SSNs and related records obtained by federal or state authorized persons pursuant to laws enacted on or after October 1, 1990, "shall be confidential, and no authorized person shall disclose any such Social Security account number or related record."

Because West Virginia law requires that all state executive branch agencies safeguard all SSNs and treat them as confidential, with disclosure as authorized by law, W. Va. Code §§ 5A-8-21 to -22, the only additional requirement yielded by this federal statute is with regard to the prohibition on disclosure.

The Attorney General of Oregon has interpreted this prohibition on disclosure to simply mean that there can be no unauthorized re-disclosure. 47 Or. Op. Atty. Gen. 1, 37, 1993 WL 602063 (Or. A.G. 1993). An authorized re-disclosure includes a re-disclosure with the individual's informed consent. Therefore, if an individual who receives a legally sufficient Privacy Act Notice discloses his or her SSN to the Department and thereby consents to the uses and disclosures identified in the notice, the Department may re-disclose the SSN per the Notice.

Unauthorized willful disclosures of SSNs and related records are felonies and punishable by fines and/or imprisonment.

Implications:

- Departments shall assess where they are disclosing SSNs.
- Departments shall adopt policies and procedures ensuring that they only disclose SSNs in accordance with their legally sufficient Notices.
- Departments shall safeguard SSNs and keep them confidential.

Source:

42 U.S.C. § 405 – Evidence, procedure, and certification for payments
http://www.law.cornell.edu/uscode/text/42/405

W. Va. Code § 5A-8-21 – Limitation on release of certain personal information maintained by state agencies and entities regarding state employees
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=8&section=21#08

W. Va. Code § 5A-8-22 – Personal information maintained by state entities
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=8&section=22#08

Principles:

Consent, Minimum Necessary and Limited Use, Security Safeguards

1.3.1. Federal Tax Return Information

IRC §§ 6103(p)(4), 7213 and 7213A
IRS Publication 1075

Description:

The Internal Revenue Code (IRC) makes information pertaining to a taxpayer's identity and tax return information confidential. Criminal penalties are imposed for the unauthorized disclosure of federal income tax returns or federal return information. Additionally, the unauthorized inspection of federal tax returns or return information is a crime. These crimes are felonies or misdemeanors depending upon the crime committed, and, upon conviction, the person may be fined or imprisoned or both fined and imprisoned.

The Commissioner of Internal Revenue is authorized to enter into exchange of information agreements with state revenue departments. Those departments and their employees are subject to the same confidentiality requirements for federal tax returns and return information as are imposed on the Internal Revenue Service and its employees.

Additionally, contractors with either the Internal Revenue Service (IRS) or a state revenue agency that have access to federal returns and return information in order to perform the contracts are subject to the same confidentiality rules and criminal provisions applicable to employees of the Internal Revenue Service or the state revenue agency.

In October 2014, the IRS issued Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, to promote taxpayer's confidence in the IRS. Publication 1075 employs specific requirements for safeguarding Federal Tax Information (FTI), which consists of federal tax returns and return information that are in the agency's possession or control. These safeguards ensure that personal and financial information furnished to the IRS will be protected against unauthorized use, inspection, or disclosure by those federal, state, and local agencies receiving FTI.

Under Publication 1075, all federal, state, and local agencies authorized to receive FTI must implement managerial, operational, and technical security controls required under Publication 1075. This ensures that FTI is adequately protected at all points where it is received, processed, stored, and transmitted.

Before the IRS will authorize an agency to access FTI, the agency must submit a Safeguard Security Report (SSR) to the IRS Office of Safeguards, evidencing that adequate safeguard protections and controls are in place. The initial SSR must be submitted for approval at least 90 days prior to receiving FTI. As part of the SSR, the agency must select a Point of Contact (POC) within the agency to serve as a liaison between the agency and the IRS. The POC is responsible for ensuring that annual internal inspections are conducted, for submitting required safeguard

reports to the IRS, for properly reporting any data breach incidents, and for any other necessary liaison activities with the IRS. The Office of Safeguards will review the SSR and authorize the agency to access FTI. Once an agency is authorized, it is responsible for updating and submitting an annual SSR to reflect any changes that impact the protections of FTI.

Additionally, when an agency plans to implement a data warehouse containing FTI, the agency must provide a written notification to the IRS Office of Safeguards 45 days prior to implementation explaining its data warehouse plans for compliance. The agency shall define how activities will occur and develop a process or policy to ensure that data warehousing security meets the baseline security requirements. More specifically, the agency's process and policy must ensure FTI will not be at risk and provide a method of informing management, defining accountability, and addressing security issues.

Authorized agencies are required to implement a standardized recordkeeping system of all requests for FTI. The records must identify and track both electronic and non-electronic FTI from creation to destruction. Moreover, the records must track internal requests among employees as well as requests from outside the agency, tracking the complete movement of FTI, to ensure the FTI is safeguarded from improper disclosures.

Publication 1075 requires suspected security incidents or potential data breach incidents of FTI to be reported by the agency. Upon discovering a possible improper inspection or disclosure of FTI, the individual making the observation or receiving information must immediately contact the special agents-in-charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguard no later than 24 hours after discovery.

Although the agencies handling FTI are responsible for fully understanding and complying with these requirements, the September 2016 update to Publication 1075 requires agencies to submit to an on-site safeguard review by an IRS inspector. During the on-site review process, the IRS evaluates the agencies' compliance with the safeguard requirements. The on-site review requires opening conferences and an actual observation of operations. The review is followed by a closing conference and issuance of Preliminary Findings Report (PFR), where the agency is immediately informed about the on-site findings. A Safeguard Review Report (SRR) and Corrective Action Plan (CAP) are then issued within 45 days to document the on-site review findings.

These reports—the PFR, SRR, SSR, and CAP—are property of the IRS. Therefore, to prevent any disclosure of data that would put FTI at risk, agencies may not disclose reports to anyone outside of the agency without express permission of the IRS.

Finally, agencies seeking to expand their technological capacities through virtual environments and cloud computing solutions must take special care to limit the associated risk. Proper safeguards must ensure that FTI remains isolated and secure.

Implications:

- Departments that have federal tax return information provided by the Internal Revenue Service must preserve the confidentiality of that information and ensure that there is no unauthorized disclosure.

- Departments that receive, possess, store or transmit Federal Tax Information must implement and follow Publication 1075 safeguard requirements to protect taxpayers' confidentiality.

See Section 3.9 for State Law on Tax Returns and Return Information.

Source:

26 U.S.C. § 6103 – Confidentiality and disclosure of returns and return information
http://www.law.cornell.edu/uscode/text/26/6103

26 U.S.C. § 7213 – Unauthorized disclosure of information
http://www.law.cornell.edu/uscode/text/26/7213

26 U.S.C. § 7213A – Unauthorized inspection of returns or return information
http://www.law.cornell.edu/uscode/text/26/7213A

IRS Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies (Updated October 1, 2014)
http://www.irs.gov/pub/irs-pdf/p1075.pdf

Additional Requirements for Publication 1075 (Updated September 30, 2016)
http://www.irs.gov/uac/Additional-Requirements-for-Publication-1075

Publication 1075 – Tax Information Security Guidelines For Federal, State, and Local Agencies (Updated September 30, 2016) https://www.irs.gov/pub/irs-utl/p1075.pdf

Principles:

Confidentiality, Minimum Necessary and Limited Use, Security Safeguards, Notice

1.4. Health Insurance Portability and Accountability Act of 1996, ("HIPAA")

Pub. L. No. 104-191

Description:

The HIPAA statute provides for the establishment of standards and other requirements for transmitting electronic health information to improve the efficiency and effectiveness of the health care system while safeguarding patient privacy and maintaining security of the health information. The HIPAA Statute mandates Federal privacy protections for individually identifiable health information. Similarly, the HIPAA statute provides for national standards for protecting the confidentiality, integrity, and availability of electronic protected health information (ePHI). (*See* Sections 1.4.1 and 1.4.2 for HIPAA Privacy Rule and HIPAA Security Rule discussions).

The Office for Civil Rights administers and enforces the HIPAA Privacy Rule and the HIPAA Security Rule.

Other HIPAA Administrative Simplification Rules are administered and enforced by the Centers for Medicare and Medicaid Services and include: (1) Transactions and Code Set Standards; (2) Employer Identifier Standard; and (3) National Provider Identifier Standard.

HIPAA was amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"). Subtitle D of the Act amends HIPAA Privacy and Security Rules. The development of health information technology (electronic health records, personal health records, health information exchanges) has resulted in additional risks; HITECH builds on HIPAA's Privacy and Security Rules to address these new risks. On January 25, 2013, OCR published an Omnibus Final Rule entitled "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules," which was modified by the "Technical Corrections to the HIPAA Privacy, Security and Enforcement Rules" final rule effective June 7, 2013 (together, the "Final Rule"), that implements a number of provisions of HITECH. The Omnibus Final Rule was effective on March 26, 2013, and required compliance as of September 23, 2013, in most instances.

For further discussion of HIPAA Breach Notification Rule *see* Section 1.4.3.

The HIPAA Statute also has an Enforcement Rule to implement standards for the enforcement of all of the HIPAA Rules.

Implications:

See listing of Implications under each Rule in Sections 1.4.1 through 1.4.3

Source:

Pub. L. No. 104-191 – Health Insurance Portability and Accountability Act of 1996
https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996

HHS HIPAA Portal
http://www.hhs.gov/ocr/privacy/

Principles:
Accountability, Notice, Minimum Necessary and Limited Use, Consent, Individual Rights, Security Safeguards

1.4.1 HIPAA "Privacy Rule"

45 C.F.R. §§ 160 and 164

Description:

The Privacy Rule became effective April 14, 2003, and applies to Covered Entities which include health plans, health care clearinghouses, and health care providers who conduct covered health transactions electronically (including submitting claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which the Department of Health and Human Services ("HHS") has established standards under the HIPAA Transactions Rule). This Rule provides a foundation of federal protections for the privacy of protected health information ("PHI") in any medium, including electronic records, paper records, and verbal communications. The Rule does not replace State law that grants individuals even greater privacy protections. The Rule covers uses and disclosures of PHI, authorizations, minimum necessary use and disclosure, workforce policies, patients' rights, organizational matters, legal matters, and safeguards.

The Privacy Rule regulations detail requirements for HIPAA Privacy Notices provided by Covered Entities that maintain a website that provides information about the Covered Entity's customer services or benefits. In such instances, privacy practices must be prominently posted on the website, and a link to the full privacy notice must be available through the website. The Office for Civil Rights ("OCR") enforces the Privacy Rule. There are civil and criminal penalties for noncompliance.

HITECH extends certain HIPAA requirements to Business Associates. The Final Rule expanded the definition of Business Associates to include patient safety organizations, health information organizations, and subcontractors. The HIPAA requirements, which were formerly imposed on Business Associates only through contracts with Covered Entities, are directly applied to Business Associates by law. However, these requirements must also be included in contracts between Covered Entities and Business Associates. Business Associates are subject to HIPAA security requirements for administrative, physical, and technical information safeguards, as well as most HIPAA privacy requirements. Pursuant to the Final Rule, Business Associates are now required to enter into written agreements with HIPAA-covered subcontractors containing satisfactory assurances from such subcontractors that PHI will be appropriately safeguarded. In addition, Business Associates are required to detect and report security breaches to Covered Entities. Finally, Business Associates are subject to civil and criminal penalties for violating their obligations under HIPAA.

Covered Entities may use and disclose PHI without a patient's written consent or authorization for the Covered Entity's own treatment, payment, and health care operations activities. Additionally disclosure is permissible absent consent where the disclosure is for the treatment activities of another health care provider, the payment activities of another Covered Entity and another health care provider; or

the health care operations of another Covered Entity (so long as the PHI pertains to a relationship both have with the individual, is the minimum necessary and the health care operations are limited to (1) quality assessment, (2) review of the quality or competence of health professionals, or (3) fraud or abuse detection or compliance). However, Covered Entities must meet the minimum necessary standard by making reasonable efforts to use and disclose only the minimum amount of PHI. Psychotherapy notes must never be disclosed without written authorization.

Covered Entities must permit an individual to request a restriction of certain uses or disclosures of PHI: (1) to carry out treatment, payment or health care operations or (2) to persons involved in the individual's care. Covered Entities are not required to agree to such requests but must abide by them, except for emergency situations. Covered Entities must comply with an individual's request to restrict the disclosure of PHI if the disclosure is to a health plan for payment or health care operations and if the PHI pertains solely to a health care item or service that has already been paid in full, out of pocket by the individual or by a person other than the health plan. The Final Rule clarified that Covered Entities may terminate a restriction upon notice to an individual, but Covered Entities may not unilaterally terminate a mandatory restriction of disclosure of PHI to a health plan if the requirements set forth above are met.

In situations where the "minimum necessary" standard applies, Covered Entities must limit the disclosure of PHI to, if possible, a Limited Data Set, or if not practicable, to the minimum necessary to accomplish the intended purpose of the disclosure. The Covered Entity or Business Associate disclosing the PHI must determine what information is minimally necessary to meet the need.

Although OCR published their Omnibus Final Rule to modify the Privacy Rule under HITECH, the rule left out one important provision of HITECH concerning amendments to the procedure and requirements for accounting of disclosures in 45 C.F.R. § 164.528. HITECH provides that if a Covered Entity uses or maintains EHR, individuals are entitled, upon request, to an accounting of disclosures for treatment, payment, and health care operations that occurred during the three years prior to the request. A Covered Entity may respond to an individual's accounting request in one of two ways: (1) provide an accounting of all disclosures made by the Covered Entity and its Business Associates or (2) provide a list of the Covered Entity's disclosures and a list of all Business Associates. Business Associates must then supply a list of disclosures upon request from the individual if the Business Associate maintains a Designated Record Set as defined by the HIPAA Privacy Rule. While the current language of Section 164.528 mandates accounting for six years and excludes treatment, payment, and health care operations, OCR is working on a final rule to implement the above portion of HITECH that was not included in the Omnibus Final Rule.

A Covered Entity or a Business Associate may not sell EHR or PHI without authorization from the individual unless (1) the information is to be used for public health activities, research or treatment; (2) there is a sale, transfer, merger or consolidation of all or part of the Covered Entity with another Covered Entity; (3) the price covers the Business Associate's cost to produce the information at the request of the Covered Entity; or (4) the price covers the cost to provide the individual with a copy of his or her PHI.

The Final Rule expanded individuals' rights to request access to electronically maintained PHI regardless of whether a particular data set is an electronic health record ("EHR"). Pursuant to 45 C.F.R. § 164.524, if an individual requests electronic copies of PHI that are stored electronically, Covered Entities must now provide them in the requested form and format, if they are readily producible as such. If they are not readily producible, the Covered Entity is required to provide a readable electronic form agreed upon with the individual. OCR expects this readable electronic form to be machine readable so that it can be analyzed by computer; acceptable forms include Word, Excel, and text-based PDF. An individual can also designate a third party recipient of e-PHI, and under the Final Rule, the Covered Entity must transmit the requested information directly to the third party as long as the individual's request (1) is in writing, (2) is signed by the individual, and (3) clearly identifies the third party and where to send the requested information. Reasonable cost-based fees may be charged for providing copies of PHI pursuant to an individual's right to access. Such fees may not exceed the cost of labor to process the request and the cost of supplies. The Final Rule clarifies that such fees do not include retrieval fees.

HITECH requires that the Secretary formally investigate if a preliminary investigation of the facts of a complaint indicate the possibility that the violation was a result of willful neglect. If willful neglect is found to have occurred, the Secretary must impose mandatory penalties. HITECH also increases the civil penalties for willful neglect. These penalties can extend up to $250,000, with repeat or uncorrected violations extending up to $1.5 million. Additionally, HITECH authorizes the State Attorney General to bring a civil action on behalf of state residents, as *parens patriae*, to enjoin violations and to obtain damages and attorney fees.

In April 2015, The Office of the National Coordinator for Health Information Technology published Version 2.0 of the "Guide to Privacy and Security of Electronic Health Information" to assist Covered Entities and Business Associates with their compliance obligations under the Privacy Rule.

In February 2016, modifications to the Privacy Rule were made to expressly permit a small subset of Covered Entities to disclose to the National Instant Criminal Background Check System the identities of individuals already prohibited by Federal law from firearm ownership for mental health reasons. The new modification only applies to Covered Entities that function as repositories of

information relevant to the Federal mental health prohibition on behalf of a State or that make mental health determinations such as commitment to a mental institution or adjudication as a mental defective. The modifications seek to dispel any uncertainty about such disclosures rather than a substantive change in the Privacy Rule.

Implications:

- Departments have completed their HIPAA assessment and implementation and are in the compliance phase. If any Department has not completed its assessment, please contact the State Privacy Office.
- Any Department that undertakes a new health-related responsibility should complete a HIPAA Covered Entity Assessment.
- HIPAA covered agencies must ensure that they have policies, procedures and Business Associate Agreements to carry out the Privacy Rule's requirements and that they have trained their workforce as appropriate.
- Business Associate Agreements must be in compliance with the Final Rule by September 23, 2013; *however*, Business Associate Agreements in effect prior to January 25, 2013 and not renewed or modified between March 26, 2013, the effective date, and September 23, 2013, the compliance date, need not be in compliance with the Final Rule Business Associate Agreement requirements until September 22, 2014. The provisions included in the Final Rule will likely require modifications to Business Associate Agreements in effect prior to the implementation of the Final Rule.
- Business Associates are subject to certain HIPAA privacy provisions, as well as sanctions for violation of Business Associate requirements. Business Associates Agreements will need to be modified to reflect these changes. *See* Section 4.0, West Virginia HIPAA Addendum.
- Business Associates are now required to obtain satisfactory assurances from subcontractors regarding safeguarding of PHI.
- Consumers must be notified of data security breaches involving "unsecured" PHI. Both Covered Entities and Business Associates must comply with these notice requirements, although the latter's notification obligation runs to the Covered Entity. *See* Section 1.4.3.
- Vendors of personal health records and their service providers are now subject to the security breach notification requirement. Individuals may prohibit Covered Entities from disclosing certain self-pay services to health plans.
- Limited data sets are the new default for PHI disclosures governed by the minimum necessary standard.
- Covered Entities using EHRs may include all disclosures of PHI for treatment, payment, and health operations in the past three (3) years when an individual requests an accounting. (*Note:* accounting of disclosures final rule was expected to be published in 2015 but the actual publication date remains uncertain.).
- Upon request, Covered Entities must provide an individual with PHI in electronic form or format requested, and transmit it to a designated third

party upon a request from the individual that (1) is in writing, (2) is signed by the individual, and (3) clearly identifies the third party and where to send the requested information.

- HIPAA covered agencies should review the HIPAA Privacy Rule requirements and its amendments needed to engage in compliance activities to ensure that the HIPAA Privacy Rule provisions are met and updated.
- Business Associates must keep a HIPAA-compliant log of certain disclosures of PHI for each individual's PHI, which includes disclosures resulting from a breach.
- Departments should ensure that their policies and procedures reflect the changes included in the Final Rule.

Source:

HHS HIPAA Portal
http://www.hhs.gov/ocr/privacy/

HIPAA Privacy Rule History
http://www.hhs.gov/hipaa/for-professionals/privacy/index.html
45 C.F.R. Part 160 – General Administrative Requirements
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfr160_main_02.tpl

45 C.F.R. Part 164 – Security and Privacy
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl

78 Fed. Reg. 5566 – Final Rule
http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

Guide to Privacy and Security of Electronic Health Information
http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

81 Fed. Reg. 382 – Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the National Instant Criminal Background Check System (NICS)
https://federalregister.gov/a/2015-33181

Principles:

Accountability, Notice, Minimum Necessary and Limited Use, Consent, Individual Rights, Security Safeguards

1.4.2. HIPAA "Security Rule"
45 C.F.R. §§ 164.302-318

Description:
The HIPAA Security Rule, published by the Department of Health and Human Services (HHS), describes what "Covered Entities" *must* do to make sure patients' electronic medical files are secure. The Security Rule is in effect for all entities. The HITECH Act amends the Security Rule and makes certain portions of the Rule directly applicable to Business Associates of a Covered Entity; the additional requirements must be set forth in the Business Associate Agreement.

The Security Rule is important to patients because, like the Privacy Rule, it creates a national standard for protecting the confidentiality, integrity, and availability of ePHI. This means that all health care providers, health plans, and health care clearinghouses that transmit information electronically must adopt a data security plan.

Only health information maintained or transmitted in electronic format is covered by the Security Rule; thus, paper records stored in filing cabinets are not subject to the security standards. For example, e-PHI includes telephone voice response and fax back systems because these systems may be used as input and output devices for electronic systems. However, it does not include paper-to-paper faxes, video teleconferencing, or messages left on voicemail because the information being exchanged did not exist in electronic format prior to transmission.

The Security Rule, according to HHS, is designed to be flexible, establishing a security framework. All Covered Entities must have a written security plan. As set forth in the Final Rule, in determining which security measures to use, a Covered Entity or Business Associate should take the following into account: (i) its size, complexity, and capabilities and (ii) its technical infrastructure, hardware, and software security capabilities. HHS identifies the following three components as necessary for the security plan:

- Administrative safeguards
- Physical safeguards
- Technical safeguards

Each of the three major categories has a number of additional subcategories, and several of the subcategories related to administrative safeguards were modified or supplemented by the Final Rule, including but not limited to risk analysis, sanction policies related to employees who fail to follow the security plan, and identification of the individual responsible for the development and implementation of required security policies. In addition to the required components, other factors are "addressable" items that should be considered and adopted if suitable to the Covered Entity's size and organization. Continuing education is among the addressable factors set forth in the Security Rule as part of rule compliance. This

includes periodic security updates. The continuing evaluation process should be developed and implemented to maintain sustainability of HIPAA Security compliance. Systematic and controlled reviews of changes that affect data security are necessary for a comprehensive evaluation program. Each Department must identify, train, and assign individuals to key processes associated with technology and operations changes.

Entities are required under the Security Rule to conduct risk analyses to implement the required security standards. On July 14, 2010, the United States Department of Health and Human Services, Office of Civil Rights ("OCR"), issued a "Final Guidance on Risk Analysis Requirements under the HIPAA Security Rule" designed to assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of ePHI. The Guidance provides sample questions an organization may wish to consider in implementing the Security Rule:

- Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain or transmit.
- What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain, or transmit e-PHI?
- What are the human, natural, and environmental threats to information systems that contain e-PHI?

The Guidance contains additional discussion of steps to assess and safeguard e-PHI. The Security Rule requires Covered Entities to adopt "incident" reporting procedures. According to HHS, the Security Rule does not specifically require any incident reporting to outside entities.

In April 2015, The Office of the National Coordinator for Health Information Technology published Version 2.0 of the "Guide to Privacy and Security of Electronic Health Information" to assist Covered Entities and Business Associates with their compliance obligations under the Security Rule.

Implications:

- Ensure the confidentiality, integrity, and availability of all e-PHI that the Covered Entity creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of e-PHI.
- Protect against any reasonably anticipated uses or disclosures of e-PHI that are prohibited by the HIPAA Privacy Rule.
- Ensure compliance by the Workforce.
- Develop methods and procedures for continuing evaluation to maintain sustainability of HIPAA Security compliance.
- Establish procedures for periodic evaluation of implemented security measures.

- HIPAA Covered Entities and Business Associates should develop a plan to revise their Business Associate Agreements to reflect any changes set forth in the Final Rule by September 23, 2014.
- Enforcement of HIPAA security provisions will be stricter with the possibility of larger civil penalties and State Attorney General enforcement.

Note:

Pursuant to the Code of Federal Regulations establishing Conditions for Federal Financial Participation, 45 C.F.R. § 95.621, Departments are responsible for the security of all automated data processing systems involved in the administration of HHS programs, and they are also responsible for the establishment of a security plan that outlines how software and data security will be maintained. This section further requires that Departments conduct a review and evaluation of physical and data security operating procedures and personnel practices on a biennial basis. CMS issued a letter to state Medicaid directors dated September 20, 2006, which specifically requires state agencies and their Business Associates to comply with the HIPAA Security requirements. In addition, CMS is requiring that all contracts include a provision requiring contractors to report breaches of privacy or security to the state Medicaid staff. The state is then obligated to report the breach to CMS.

Implications/Best Practices:

- Departments must remember that risk mitigation is the compliance objective.
- Security plans should present Department security features and requirements in terms of their risk mitigation benefits.
- Department security plans should document the risk mitigation rationale and effectiveness.
- Departments must balance the cost-effective dollar arguments against the higher obligation to ensure patient privacy and safety.
- Develop procedures to keep privacy and security concerns coupled.
- Departments who receive federal funding should check with their federal funder for additional requirements.
- Departments with HIPAA Business Associate Agreements must evaluate and confirm compliance with the Security Rule as Business Associates are now subject to HIPAA's (increased) civil and criminal penalties.

Source:

Final Rule ePHI Security Standards
http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf

HIPAA Security Rule History
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

Guidance on Risk Analysis
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

78 Fed. Reg. 5566 – Final Rule
http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

Guide to Privacy and Security of Electronic Health Information
http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Principles:
Security Safeguards, Notice, Accountability

1.4.3. HIPAA Breach Notification Rule

Description:

On January 25, 2013, OCR published an Omnibus Final Rule entitled "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other changes to the Interim Final Rule for Breach Notification." The Final Rule became effective on September 23, 2013.

The Breach notification requirements apply if all of the following are present:

- There is a "Breach." The Final Rule defines "Breach" to mean the unauthorized acquisition, access, use, or disclosure of PHI. The definition of "Breach" excludes (i) the unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a Covered Entity or Business Associate, (ii) inadvertent disclosure of PHI from a person authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the Covered Entity or Business Associate, and (iii) disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that the unauthorized person to whom disclosure was made would not have reasonably been able to retain the information.
- The PHI is "unsecured." The Rule defines "unsecured protected health information" to mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS guidance.
- The Breach "compromises the security of the PHI." Pursuant to the Final Rule, an unauthorized acquisition, access, use, or disclosure of PHI is presumed to be a Breach unless the Covered Entity or Business Associate demonstrates, based on a risk assessment, that there is a low probability that the PHI has been compromised. The risk assessment should be based upon, but not limited to, the following factors: (i) the nature and extent of health information involved, (ii) the unauthorized person who used the PHI or to whom the PHI was disclosed, (iii) whether the PHI was actually acquired or viewed, and (iv) the extent to which the risk has been mitigated. HHS also noted that it may be appropriate to consider other information depending on the particular circumstances.

There is no requirement of actual harm in order to trigger notification. A Breach is considered to be discovered as of the first day the Breach is known to the Business Associate or Covered Entity. All required notifications must be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the Breach by the Covered Entity or Business Associate.

The regulations, developed by OCR, require health care providers and other Covered Entities to promptly notify affected individuals of a Breach, as well as the HHS Secretary and the media in cases where a Breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary no later than 60 days after the end of the calendar year in which the Breaches were discovered. The regulations also require Business Associates of Covered Entities to notify the Covered Entity of Breaches at or by the Business Associate.

The definition of a Breach, the content of the notice and method of delivery contained in the HIPAA Security Rule are similar to comparable provisions in West Virginia's breach notification law. *See* Section 3.18.

In April 2015, The Office of the National Coordinator for Health Information Technology published Version 2.0 of the "Guide to Privacy and Security of Electronic Health Information" to assist Covered Entities and Business Associates with their compliance obligations under the Breach Notification Rule.

Note:
The Federal Trade Commission (FTC) issued companion breach notification requirements for vendors of personal health records (PHRs) and their third party service providers following the discovery of a breach of unsecured PHR-identifiable health information. For further discussion, *see* Section 1.6. Entities operating as Covered Entities and Business Associates are technically not subject to the FTC breach notification rules. (*See* Section 1.6.1 for further discussion). But in certain instances where a breach involves an entity providing PHRs to customers of a Covered Entity through a Business Associate arrangement, and directly to the public, the FTC will deem compliance with the HHS Rule as compliance with its own breach notification rules.

HHS has emphasized that this Rule does not modify a Covered Entity's responsibilities with respect to the HIPAA Security Rule nor does it impose any new requirements upon Covered Entities to encrypt all PHI. A Covered Entity may still be in compliance with the Security Rule even if it decides not to encrypt electronic PHI so long as it utilizes another method to safeguard information in compliance with the Security Rule. However, if such method is not in compliance with the requirements of the Rule with respect to securing PHI, then the Covered Entity will be required to provide a breach notification to affected individuals upon a breach of unsecured PHI. The Rule preempts contrary State breach notification laws. A Covered Entity must still comply with requirements of State law which are in addition to the requirements of the Rule, but not contrary to such requirements (such as additional elements required to be included in a notice). *See* Section 3.18, West Virginia Breach Notification Law.

Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

On April 19, 2009, HHS issued "Guidance" on technologies that protect health information. To determine when information is "unsecured" and notification is required by the HHS and FTC rules, the guidance specifies encryption and destruction technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals, and therefore "secured." Entities subject to the HHS and FTC regulations that secure health information as specified by the guidance through encryption or destruction are relieved from having to notify in the event of a breach of such information.

According to the Guidance, PHI is rendered unusable, unreasonable, or indecipherable to unauthorized individuals only if one or more of the following methods are used:

(1) *Encryption*. Electronic PHI is only secured where it has been encrypted. The HIPAA Security Rule specifies encryption to mean the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. The Rule identifies the various encryption processes which are judged to meet this standard. Such confidential process or key that might enable decryption must not have been breached. To avoid a breach of the confidential process or key, decryption tools should be kept on a separate device or at a location separate from the data they are used to encrypt or decrypt.

(2) *Destruction*. Hard copy PHI, such as paper or film media, is only secured when it has been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Electronic media is secured when PHI can no longer be retrieved from it because the media has been cleared, purged, or destroyed consistent with National Institute of Standards and Technology (NIST) guidelines.

Implications:

- Departments will assess and determine the types of information they maintain that must be "secured" and will evaluate whether the use of encryption technology is appropriate.
- Departments will develop and implement destruction policies pertaining to media containing PHI.
- Departments will develop and update in accordance with the Final Rule policies and procedures for determining whether a breach has occurred. Issues to cover include:
    - Steps for identifying a potential breach incident.
    - Steps for determining whether the incident is an impermissible use or disclosure of PHI under the HIPAA Privacy Rule.

- Steps for performing a risk assessment analysis based upon the factors set forth in the Final Rule.
- Steps to ensure that affected individuals, the media and/or HHS receive proper notification, as required.
- Documentation for each step of these processes.
- Discussion of the new policies and procedures with the employer's HIPAA privacy officer, who will be responsible for this additional enforcement.

- Departments will work with each Business Associate regarding implementation of policies and procedures relating to breach notification. Issues to cover include:
  - Requesting a copy of the security breach notification policies and procedures that the Business Associate will implement.
  - Discussing the reporting of security incidents and breaches to the Covered Entity.
  - Discussing the difference between reportable and non-reportable breaches.
  - Determining the role of the Business Associate in identifying breaches and suspected breaches related to the Business Associate's service agreement.
  - Allocating responsibility for fulfilling the notification requirements when a reportable breach has occurred and maintaining any related data required under the interim final rule.
  - Amending the indemnification provisions of the Business Associate Agreement to ensure that the appropriate party bears the costs associated with the notification requirements and liability for failure to comply with them.

Source:
Breach Notification Rule
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html
78 Fed. Reg. 5566 – Final Rule
http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

Guide to Privacy and Security of Electronic Health Information
http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Principles:
Notice, Security Safeguards

1.5. The Affordable Care Act; Affordable Insurance Exchanges

45 C.F.R. Parts 155, 156 and 157

Description:

The Patient Protection and Affordable Care Act of 2010 as amended by the Health Care and Education Reconciliation Act of 2010, collectively known as the Affordable Care Act ("ACA"), provides for states to create affordable insurance exchanges to provide competitive marketplaces for individuals and small business employers to directly compare available private health insurance options on the basis of price, quality and other factors. Some have questioned whether or not and to what extent these new exchanges will be subject to the Privacy Act and the HIPAA Security Rule previously discussed in Sections 1.4..1-2.

On March 27, 2012, HHS published a final rule entitled "Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans; Exchange Standards from Employers" ("ACA Final Rule"). The ACA Final Rule implements the affordable insurance exchange provisions and requirements of the ACA and took effect on May 29, 2012. The final rule provides three options for states to adopt insurance exchanges. States may establish an exchange that facilitates qualified health plans (QHPs) as well as a small business health options program (SHOP), establish an exchange which only facilitates a SHOP, or partner with the federal government. West Virginia has elected to participate in the State Partnership Exchange model whereby the Federal Exchange is utilized but continues to benefit from state recommendations and interaction with issuers and consumers.

Section 155.260 of the ACA Final Rule provides for the privacy and protection of personally identifiable information collected by an exchange. Where the exchange creates or collects personally identifiable information for the purpose of determining eligibility for enrollment in a qualified health plan, determining eligibility for other insurance affordability programs, or determining exemptions from the individual health insurance mandate, the exchange may only use or disclose the personally identifiable information if necessary for several reasons. The exchange may use or disclose the personally identifiable information to carry out its functions as described in section 155.200 of the ACA Final Rule. With the consent of an individual, the exchange may also use or disclose the information to ensure the efficient operation of the exchange or to determine eligibility to enroll in the Marketplace, claim a premium tax credit, or claim a cost-sharing reduction.

The exchange may not create, collect, use or disclose personally identifiable information while the exchange is fulfilling its responsibilities under section 155.200 unless the creation, collection, use or disclosure are consistent with section 155.260.

The exchange must establish and implement privacy and security standards that are consistent with the following principles laid out in section 155.260: individual

access, correction, openness and transparency, individual choice, limitations, data quality and integrity, safeguards, and accountability. For purposes of implementing the security safeguards and preventing the improper use or disclosure of personally identifiable information as required by section 155.260, the exchange must establish and implement certain operational, technical, administrative and physical safeguards that are consistent with Section 155.260 and any other applicable law. On February 29, 2015, the Centers for Medicare & Medicaid Services ("CMS") released a Final 2017 Letter to Issuers in the Federally-facilitated Marketplaces offering guidance for issuers of QHPs. It requires that all Federally-facilitated Marketplaces meet certain requirements by 2017. The exchange must submit a Privacy and Security Agreement along with a Senior Officer Acknowledgement to CMS setting out provisions for safeguarding privacy. Agents and brokers must also submit a Privacy and Security Agreement to CMS. The recertification process mirrors the 2016 certification process.

To the extent that the exchange performs transactions with a Covered Entity, section 155.270 of the ACA Final Rule requires exchanges to use standards, implementation specifics, operating rules, and code sets adopted by the Secretary of HHS pursuant to HIPAA or that are otherwise approved by HHS.

Implications:

The West Virginia Health Insurance Exchange is subject to the requirements of this new federal regulation.

Source:

77 Fed. Reg 18310 – Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans; Exchange Standards for Employers (Final Rule)
http://www.healthreformgps.org/wp-content/uploads/2012-6125.pdf

HHS Guidance on the State Partnership Exchange
http://www.cms.gov/CCIIO/Resources/Fact-Sheets-and-FAQs/Downloads/partnership-guidance-01-03-2013.pdf

Final 2017 Letter to Issuers in the Federally-facilitated Marketplaces by Centers for Medicare & Medicaid Services
https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Final-2017-Letter-to-Issuers-2-29-16.pdf
-

West Virginia Insurance: Latest News
http://bewv.wvinsurance.gov/LatestNews.aspx

Principles:

Confidentiality, Security and Limited Use of Personally Identifiable Information

1.6. Federal Trade Commission's Health Breach Notification Rule

16 C.F.R. Part 318

Description:

The HITECH Act and the American Recovery and Reinvestment Act of 2009 requires the Federal Trade Commission ("FTC") to implement and enforce breach notification provisions that apply to vendors of personal health records and their third-party service providers that are not otherwise subject to the requirements of HIPAA.

The FTC breach notification rule applies if you are:

- A vendor of personal health records (PHRs);
- A PHR-related entity; or
- A third-party service provider for a vendor of PHRs or a PHR-related entity.

Covered Entities and Business Associates are not technically subject to the FTC's breach notification rule but must comply with the HHS's breach notification rule. *See* Section 1.6.1 for further discussion.

Notice must be given when there is an "unauthorized acquisition" of "PHR-identifiable health information" that is "unsecured" and in a "personal health record". These terms are defined in the Health Breach Notification Rule (the "Breach Notification Rule") and the definitions of the terms are important.

If there is a security breach and you are a "vendor of personal health records" or a "PHR-related entity", the Breach Notification Rule provides the next steps that should be taken. The subject entity must notify:

1. each affected person who is a citizen or resident of the United States;
2. the FTC; and
3. the media (in cases where a breach affects more than 500 individuals).

The rule sets forth who to notify, when to notify them, how to notify them, and what information to include.

Persons: If a vendor of personal health records or a PHR-related entity experiences a breach of unsecured personal health information, each affected person should receive notice "without unreasonable delay" and within 60 calendar days after the breach is discovered. The 60 day period begins to run the day the breach becomes known to someone in the company (vendor of PHRs or PHR-related entity) or the day someone reasonably should have known about it. Those subject to the Rule must act without unreasonable delay. This means if a company discovers the breach and gathers the necessary information within 30 days, it is unreasonable to wait until the 60th day to notify the people whose information was breached.

FTC: The Rule requires notice to the FTC. The timing depends on the number of people affected by the breach:

> *500 or more people*: The FTC must receive notice as soon as possible and within 10 days after discovering the breach. The report should be provided on the FTC's form at: www.ftc.gov/healthbreach.
>
> *Fewer than 500 people*: Notice must be given, but more time is given to provide the information. The FTC form noted above must be provided with forms documenting any other breaches during the same calendar year involving fewer than 500 people within 60 calendar days following the end of the calendar year.

The Media: When at least 500 residents of a particular state, District of Columbia or U.S. Territory or possession are affected by a breach, notice must be provided to prominent media outlets serving the relevant locale, including Internet media where appropriate, without unreasonable delay and within 60 calendar days after the breach is discovered. This notice is in addition to individual notices.

Third-party service providers to a vendor of PHR or a PHR-related entity also have notice requirements under the Rule. If the third-party service provider experiences a breach, it must notify an official designated in its contract with the vendor or a senior official within the vendor company—without unreasonable delay and within 60 calendar days of discovering the breach. The Rule requires the third-party provider to identify for the vendor client each person whose information may be involved in the breach. The third-party service provider must receive an acknowledgement from the vendor client that they received the notice.

Personal notice must be provided by first-class mail to the individual at the last known address of the individual, or by e-mail, if the individual receives a clear, conspicuous opportunity to receive notification by first-class mail and does not exercise that choice. In the case of a deceased individual, notice must be provided to the next of kin if the contact information is provided along with authorization to contact them.

Substitute notice is required if the contact information for 10 or more individuals is insufficient or out-of-date. Substitute notice is accomplished by:

1. a clear and conspicuous posting for 90 days on your home page, or
2. a notice in major print or broadcast media where those people likely live.

The content of the notice should include the following:

- A brief description of what happened, including the date of the breach (if known) and the date you discovered the breach;

- The kind of PHR-identifiable health information involved in the breach. For example, insurance information, social security numbers, financial account data, dates of birth, medication information, etc.;
- Steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the entity that suffered the breach is doing to investigate the breach, mitigate harm, and protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll free telephone number and e-mail address, web site, or postal address.

The FTC will treat each violation of the Rule as an unfair or deceptive act or practice in violation of a Federal Trade Commission regulation. Businesses that violate the Rule may be subject to a civil penalty of up to $16,000 per violation.

Note:

The FTC's Rule preempts contradictory state breach notification laws, but not those that impose additional–but non-contradictory–breach notification requirements. For example, West Virginia's breach notification law requires breach notices to include advice on monitoring credit reports or contact information for consumer reporting agencies. While these content requirements are different from the FTC Rule's requirements, they are not contradictory. In this example, it is possible to comply with both federal and West Virginia requirements by including all the information in a single breach notice. The FTC Rule does not require the sending of multiple breach notices to comply with both state and federal law.

In 2015, a number of federal data privacy and breach notification bills were introduced and remain under consideration in Congress. This legislation seeks to create federal breach notification laws that would preempt current individual state privacy laws. The proposed bills generally provide enforcement power to the FTC, among other entities. Two pending bills, H.R. 2205 and S. 961, specifically exempt federal, state, and local government agencies from the definition of a covered entity, therefore the FTC would not have enforcement power over state agencies if those bills become law. The other pending legislation does not specifically address whether state government agencies are subject to the proposed legislation and whether the FTC has enforcement power over state government agencies if those bills are enacted.

Implications:

- Departments should identify a "team" to handle breach and related notifications.
- The "team" members might include the following: chief information officer, compliance officer, human resources, legal/risk management, or public relations with input from State Chief Privacy Officer.

- Departments should develop templates of policies and procedures and forms of documents compliant with the new FTC federal standard and applicable state law breach notification requirements.
- Development of an action plan, including checklists of key contacts such as media and others both inside and outside the Department, will enable Departments to effectively and timely respond to potential breach notification situations.

Source:

74 Fed. Reg. 42962 - Health Breach Notification Rule (Final Rule)
http://www.gpo.gov/fdsys/pkg/FR-2009-08-25/pdf/E9-20142.pdf

Complying with the FTC's Health Breach Notification Rule
http://business.ftc.gov/documents/bus56-complying-ftcs-health-breach-notification-rule

H.R. 2205 – Data Security Act of 2015
https://www.congress.gov/bill/114th-congress/house-bill/2205

S. 961 – Data Security Act of 2015
https://www.congress.gov/bill/114th-congress/senate-bill/961

Principles:

Notice

1.6.1. FTC Enforcement of PII and PHI Data Security of HIPAA Covered Entities and Business Associates

15 U.S.C. § 45(a)

In re LabMD, Inc., FTC Docket No. 9357, Complaint, August 28, 2013; 14-12144, D.C. Docket No. 1:14-cv-00810-WSD (11th Cir. Jan. 20, 2015).

Description:

The Federal Trade Commission (FTC) is given power "to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." "Unfair or deceptive acts or practices" includes those involving foreign commerce that "cause or are likely to cause reasonably foreseeable injury within the United States." Since the advent of electronic storage and conveyance methods, the security of health care data has become an increasing concern; traditionally, these HIPAA concerns would be addressed by the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) for entities meeting the HIPAA definition of either a Covered Entity or Business Associate (HIPAA entities). However, the FTC has begun to use its authority under 15 U.S.C. § 45 to enforce security conscious "acts and practices" within the health care industry and expand its scope of enforcement power to HIPAA entities.

By a complaint dated August 28, 2013, the FTC alleged that LabMD, Inc. had "failed to provide reasonable and appropriate security for personal information on its computer networks." LabMD was a corporation which conducted clinical laboratory tests; in its normal course of business, LabMD dealt with great amounts of personal information related to insurance, payment methods, and health records. The complaint precipitated as a result of the allegation that LabMD's billing department manager downloaded Limewire, a file sharing application, and shared hundreds of sensitive files over the internet. The FTC found that LabMD did not maintain an information protection program, identify foreseeable risks, train employees, or detect unauthorized software. Because sensitive information was made available online for an extended period of time—and was, in fact, found in the possession of individuals charged with identity theft—the FTC concluded that those failures "caused, or [were] likely to cause, substantial injury to consumers."

The FTC's resulting order involved extensive requirements and long term supervision over the company's practices. LabMD was instructed to implement a comprehensive security program and acquire third-party assessments every two years for a period of twenty years. The security program had to involve the designation of a coordinating employee, assessment of risks, implementation and regular testing of safeguards to control those risks, requirement by contract of service providers to maintain appropriate safeguards, and continuing evaluation and adjustment of safeguards. In addition to maintaining certain files for FTC inspection, the FTC required that those individuals and companies affected by the breach be notified of the events surrounding it, subsequent action, and ways to prevent identity theft. In response to LabMD's motion to dismiss, the FTC decided

that its authority to prevent unfair acts and practices extended "to a company's failure to implement reasonable and appropriate data security measures."

Based on the information in the FTC complaint, LabMD would be considered a HIPAA Covered Entity because it falls under HIPAA's definition of a health care provider; it would thus be governed by HIPAA's expansive requirements under the HIPAA Privacy and Security Rules. In response to LabMD's motion to dismiss, the FTC also rejected the contention that HIPAA precluded the commission from enforcing data security in the field of health care, claiming that there was nothing in HIPAA that would lead to that preemption. As a result of the order, LabMD has been forced to scale back its operations, has been denied insurance coverage, and is pursuing additional legal action against the FTC.

In March 2014, LabMD filed suit in the Northern District of Georgia seeking a declaratory judgment that the FTC lacks authority to regulate PHI data security. The Northern District of Georgia dismissed the suit, finding that the FTC had not yet issued a final order. In January 2015, LabMD appealed and the Court of Appeals for the Eleventh Circuit affirmed the dismissal. However, the Eleventh Circuit declined to rule on the issue of whether the FTC has authority to enforce healthcare privacy standards, and concluded that LabMD's arguments are reviewable only after the administrative proceedings are final.

In November 2015, the administrative law judge ("ALJ") issued an Initial Decision dismissing the charges after finding that FTC failed to show that LabMD's data security practices caused harm to consumers. However, the ALJ did not address whether the FTC has jurisdiction over data security issues. On July 29, 2016, the FTC issued an Opinion and Final Order reversing the Initial Decision. The FTC concluded that LabMD's practices were unreasonable in violation of Section 5 of the Federal Trade Commission Act. The FTC ruled that the ALJ "applied the wrong legal standard for unfairness," and rejected the ALJ's holding requiring a tangible harm to accompany the unauthorized exposure of sensitive medical information. In contrast to the ALJ's holding that a substantial injury be "probable," the FTC concluded that "LabMD's security practices were unreasonable, lacking even basic precautions to protect the sensitive consumer information maintained on its computer systems." The Order reinstates the requirements of the previous order. Now that a final order has been issued in this case, the Eleventh Circuit may review the issue of the FTC's authority. On August 30, 2016, LabMD requested that the FTC stay the effective date of its order until after planned court appeals are resolved.

See also In re Accretive Health, Inc., FTC Docket No. C-4432, Complaint, February 5, 2014 (issuing an order similar to that in LabMD resulting from the theft from an employee's vehicle of a company laptop containing the information of 23,000 patients); *In re GMR Transcription Services, Inc.*, FTC Docket No. C-4482, Complaint, January 31, 2014 (proposing an order similar to that in LabMD where a transcription service failed to ensure that its own employees and overseas

service provider implemented reasonable security measures, resulting in a large number of sensitive files becoming available online through a major search engine); *In re PaymentsMD*, FTC Docket No. C-4505, Complaint, December 3, 2014 (issuing an order against a HIPAA covered entity resulting from a failure to obtain adequate consent from consumers regarding collection of those consumers' medical records); *In re Henry Schein Practice Solutions, Inc.*, FTC Docket C-4575, Complaint, January 5, 2016 (issuing an order against a third-party service provider resulting from deceptive marketing claims concerning HIPAA-compliant encryption of patient information).

In each of the cases referenced above, the FTC issued a Decision and Order requiring the companies to comply with various conditions ranging from notifying affected customers; implementing comprehensive information security programs; obtaining information security assessments from qualified, objective, independent third-party professionals; and paying fines.

Implications:

- Departments should be aware that the FTC is exercising its power over unfair acts and practices to take action in cases of health data breach and inadequate consent.
- Departments should monitor the ongoing proceedings of *LabMD, Inc. v. FTC* in order to be aware of developments or determinations concerning the authority of the FTC.
- Covered Entities and Business Associates that deal with PII and PHI should consider implementing security programs that meet the standards of those laid out by the FTC in its orders.
- Covered Entities and Business Associates should ensure that their service providers maintain similar security programs.

Source:

15 U.S.C. § 45 – Unfair methods of competition unlawful; prevention by Commission
http://www.law.cornell.edu/uscode/text/15/45

45 C.F.R. § 160.103 – Definitions
http://www.law.cornell.edu/cfr/text/45/160.103

In re LabMD, Inc., FTC Docket No. 9357, Complaint, August 28, 2013
http://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter

In re LabMD, Inc., FTC Docket No. 9357, Order Denying Respondent LabMD's Motion to Dismiss
http://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter

In re LabMD, Inc., FTC Docket No. 9357, Initial Decision, November 13, 2015
https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf

In re LabMD, Inc., FTC Docket No. 9357, Final Order, July 28, 2016
https://www.ftc.gov/system/files/documents/cases/160729labmdorder.pdf

In re LabMD, Inc., FTC Docket No. 9357, Opinion of the Commission, by Chairwoman Edith Ramirez
https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf

LabMD, Inc. v FTC, 14-12144, D.C. Docket No. 1:14-cv-00810-WSD (11th Cir. Jan. 20, 2015)
https://www.ftc.gov/system/files/documents/cases/d09351labmdappealorder_0.pdf

In re Accretive Health, Inc., FTC Docket No. C-4432, Complaint, February 5, 2014.
http://www.ftc.gov/enforcement/cases-proceedings/122-3077/accretive-health-inc-matter

In re Accretive Health, Inc., FTC Docket No. C-4432, Decision and Order, February 5, 2014
http://www.ftc.gov/enforcement/cases-proceedings/122-3077/accretive-health-inc-matter

In re GMR Transcription Services, Inc., FTC Docket No. C-4482, Complaint, January 31, 2014
http://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter

In re GMR Transcription Services, Inc., FTC Docket No. C-4482, Decision and Order, August 21, 2014
https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf

In re PaymentsMD, FTC Docket No. C-4505, Complaint, December 3, 2014
https://www.ftc.gov/system/files/documents/cases/141201paymentsmdcmpt.pdf

In re PaymentsMD, FTC Docket No. C-4505, Decision and Order, December 3, 2014
https://www.ftc.gov/system/files/documents/cases/150206paymentsmddo.pdf

In re Henry Schein Practice Solutions, Inc., FTC Docket C-4575, Complaint, January 5, 2016
https://www.ftc.gov/system/files/documents/cases/160105scheincmpt.pdf

In re Henry Schein Practice Solutions, Inc., FTC Docket C-4575, Decision and Order, May 20, 2016
https://www.ftc.gov/system/files/documents/cases/160523hspsdo.pdf

Principles:
Security Safeguards; Individual Rights

1.7. Confidentiality of Substance Abuse Records, Reports of Violations

42 U.S.C. § 290dd-2; 42 C.F.R. Part 2, *et seq.*

Description:

Substance abuse records created in connection with federally assisted treatment programs are confidential. Federal assistance includes programs conducted by a federal agency; licensed, certified, registered, or otherwise authorized by a federal agency; funded by a federal agency; and assisted by the IRS through allowance of income tax deductions or through the granting of tax-exempt status to the program. Confidential information includes name, address, social security number, fingerprints, photograph, or similar information by which the identity of the patient can be determined with reasonable accuracy and speed directly or by reference to other publicly available information. The protections begin when a person applies for or has been given a diagnosis or treatment for alcohol or substance abuse at a federally assisted program; protections are extended to former and deceased patients. Use and disclosure must be limited to the minimum necessary. Disclosure may not occur without patient consent, unless an exception applies, and restrictions apply to recipients of the information. One significant exception is that alcohol and drug testing that is not conducted as part of a diagnosis of or treatment for an alcohol or other substance problem is not protected by these confidentiality rules. The regulations specify the elements that must be in the consent and the required accompanying statement. The regulations also require security, notice of privacy rights to patients, patient access, and restriction on use.

A violation of the regulations may be reported to the U.S. Attorney in the judicial district in which the violation occurs. A methadone program which is believed to have violated the regulations may be reported to the Regional Offices of the Food and Drug Administration.

There are criminal penalties for violation of these regulations.

In February 2016, SAMHSA published a proposed rule which would update and modernize the existing regulations. The new regulations concern the technological advances in the healthcare field, the advent of new models of integrated care, and the increased focus on performance measurement. The comment period ended on April, 11, 2016. SAMSHA plans to finalize this rule in 2016.

Note:

The Substance Abuse & Mental Health Services Administration (SAMHSA) and the Office of the National Coordinator (ONC) for Health Information Technology have posted Frequently Asked Questions (FAQs) for Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE). The FAQs outline the general provisions of 42 C.F.R. Part 2, provide guidance on its application to electronic health records, and identify methods for including substance abuse patient record information in health information exchange that is

consistent with the Federal statute. The FAQs are not meant to provide legal advice.

Implications:

- Departments should determine whether they receive and/or create substance abuse patient records from a federally assisted facility.
- Departments that do receive and/or create substance abuse patient records must adopt policies and procedures to ensure compliance with these regulations.
- The CPO shall forward the information regarding the security requirements to the Director of Information Security.
- Departments cannot apply W. Va. Code § 27-3-1(b)(6) as revised by H.B. 3184, effective June 08, 2007, to substance abuse records from federally assisted programs.

Departments should review the issued guidance applying the Substance Abuse Confidentiality Regulations to health information exchange and assess whether any policies or procedures should be updated.

Source:

42 U.S.C. § 290dd-2 – Confidentiality of records
http://www.law.cornell.edu/uscode/text/42/290dd-2

42 C.F.R. Part 2 – Confidentiality of Alcohol and Drug Abuse Patient Records
http://www.law.cornell.edu/cfr/text/42/2

81 Fed. Reg. 6987 – Proposed Rule
https://federalregister.gov/a/2016-01841

Substance Abuse & Mental Health Services Administration – Confidentiality Regulations
http://www.samhsa.gov/laws-regulations-guidelines/medical-records-privacy-confidentiality

SAMHSA – Frequently Asked Questions
http://www.samhsa.gov/about-us/who-we-are/laws/confidentiality-regulations-faqs

SAMHSA – Frequently Asked Questions Part II
http://www.samhsa.gov/sites/default/files/faqs-applying-confidentiality-regulations-to-hie.pdf

Principles:

Notice, Minimum Necessary and Limited Use, Consent, Individual Rights, Security Safeguards

1.8. Gramm-Leach Bliley-Act (GLB)

15 U.S.C. § 6801, 16 C.F.R. § 313; 72 Fed. Reg. 62890

Description:

Any financial institution that provides financial products or services to consumers must comply with the GLB privacy provisions. An entity has consumers if it provides financial products or services to individuals, not businesses, to be used primarily for their personal, family, or household purposes. Under the Federal Trade Commission's (FTC) Privacy Rule, a financial institution means "any institution the business of which is engaging in financial activities as described in § 4(k) of the Bank Holding Company Act of 1956 [12 U.S.C. § 1843(k)]." *See* 16 C.F.R. § 313.3(k)(1). Further, an institution is not a financial institution unless it is *significantly engaged* in financial activities. *Id.* State entities do not fall under the definition of a "financial institution" under GLB.

Financial activities generally include lending money, investing for others, insuring against loss, providing financial advice, making a market in securities, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, non-bank lenders, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors, and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors. Government entities that provide financial products such as student loans or mortgages are financial institutions that engage in financial activities. However, before GLB applies, the financial institution must be "significantly engaged" in financial activities, which is a flexible standard that takes into account all the facts and circumstances.

GLB provides privacy, safeguarding, and pretexting (regarding obtaining information under false pretenses) requirements. GLB privacy protections require initial and annual distribution of privacy notices and place limits on disclosures of nonpublic personal information. The FTC is authorized to enforce this law.

The Financial Services Regulatory Relief Act of 2006 amended the GLB to require certain federal agencies to propose a succinct, comprehensible, and easy to read model form that allows consumers to easily compare the privacy practices of different financial institutions.

Effective since January 1, 2011, financial institutions that wish to be protected under the FTC's "safe harbor" must convert to a model privacy notice. The "safe harbor" provides the financial institutions with security in that they are assured that the notice satisfies the disclosure requirements. To retain protection, the financial institution should not amend the FTC's model notice, including, without limitation, its wording or formatting. Failure to adopt the model notice does not mean that the notice is deficient but merely that it does not enjoy automatic protection. Likewise the prior "model clauses" no longer enjoy "safe harbor" protection. Financial institutions should examine their notices and policies and consider updating to the

model privacy notice. Eight federal regulators released a model consumer privacy notice online form builder to assist financial institutions in preparing acceptable forms.

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (the "Act") amended several sections of GLB giving rulemaking authority under the Act to the Consumer Financial Protection Bureau (the "CFPB") except that the CFPB does not have authority to establish financial institutions data safeguards – this remains with the FTC. Additionally, the SEC and the FTC are charged with the power to prescribe certain GLB rules for entities under their jurisdictions. Enforcement of the regulations resides with the CFPB for banks over 10 billion in assets, then with the FTC or other functional regulators. Residual jurisdiction is the FTC and the CFPB. These changes became effective on July 21, 2011.

Congress has considered new legislation since early 2013 that, if passed, could impact notice requirements under GLB. On April 13, 2015, the House of Representatives passed H.R. 601, which would exempt certain financial institutions from providing annual privacy notices required under GLB. A similar bill is pending in the Senate, S. 423, with only minor differences from the House version. This potential change to GLB section 503 would allow institutions that have not altered their policies and practices regarding disclosure of nonpublic personal information to avoid the burden of sending duplicative notices annually.

On October 28, 2014, the CFPB passed an Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act, Regulation P. This Regulation is similar to H.R. 601 and S. 423, and attempts to limit the burden the Annual Privacy Notice Requirement places on institutions. Regulation P allows institutions to post their annual privacy notices online rather than delivering them individually. However it does require that the customer acknowledge receipt of the notice electronically before obtaining a service. On June 24, 2015, the FTC published proposed amendments to its rules to permit auto dealers that finance car purchases or provide car leases to provide online updates to consumers about their privacy policies in lieu of sending yearly updates by mail. The public comment period for the proposed amendment closed on August 31, 2015, with no further action reported to date.

On July 11, 2016, the CFPB published a proposed amendment to Regulation P, which requires, among other things, that financial institutions provide an annual notice describing their privacy policies and practices to their customers. The amendment would implement a December 2015 statutory amendment to GLB providing an exception to this annual notice requirement for financial institutions that met certain conditions. The comment period for this proposed amendment closed on August 10, 2016.

Implications/Best Practices:

None. State entities do not fall under the definition of "financial institution" under GLB. Nevertheless, as a matter of creating policies for "best practices," it may be useful to consider the following implications that apply to "financial institutions":

- Entities must assess whether they are significantly engaged in financial activities.
- If applicable, financial institutions must develop policies and procedures to ensure an initial and annual notice is distributed and that there are limits on disclosure of nonpublic personal information.
- Financial institutions may rely on the Model Privacy Form as a safe harbor to provide disclosures under the GLB privacy rule.
- The CPO shall forward the information regarding the safeguard requirements to the Director of Information Security.

See Section 3.8 for the Maxwell Governmental Access to Financial Records Act, which governs when financial institutions may disclose a consumer's records to a state entity.

Source:

15 U.S.C. § 6801 – Protection of nonpublic personal information
http://www.law.cornell.edu/uscode/text/15/6801

FTC – Gramm-Leach-Bliley Act Legal Resources
http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act

16 C.F.R. Part 313 – Privacy of Consumer Financial Information (Privacy Final Rule)
https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/privacy-consumer-financial-information

SEC Fact Sheet – What Does [Name of Financial Institution] Do With Your Personal Information?
http://www.sec.gov/rules/final/2009/34-61003_modelprivacyform_nooptout.pdf

Federal Reserve Bank – Instructions for using the Privacy Notice Online Form Builder
http://www.federalreserve.gov/bankinforeg/privacy_notice_instructions.pdf

Privacy of Consumer Financial Information – Regulation P, 12 C.F.R. § 1016
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=c677e9290858157edaa598c5957f44d2&tpl=/ecfrbrowse/Title12/12cfr1016_main_02.tpl

Proposed Amendment to Regulation P, 12 C.F.R. § 1016
https://www.regulations.gov/document?D=CFPB-2016-0032-0001

S. 423 – Privacy Notice Modernization Act of 2013

https://www.congress.gov/bill/114th-congress/senate-bill/423/all-info

H.R. 601 – Eliminate Privacy Notice Confusion Act
https://www.congress.gov/bill/114th-congress/house-bill/601

Principles:
Notice, Consent, Minimum Necessary and Limited Use, Security Safeguards

1.8.1. Gramm-Leach-Bliley Act (GLB), "Safeguards Rule"

15 U.S.C. §§ 6801-09; 16 C.F.R. § 314

Description:

The Safeguards Rule, which implements the security requirements of the GLB, requires financial institutions to have reasonable written policies and procedures to ensure the integrity and confidentiality of customer information. State entities do not fall under the GLB definition of a "financial institution."

The Rule is intended to be flexible to accommodate the wide range of entities covered by GLB, as well as the wide range of circumstances entities face in securing customer information. Accordingly, the Rule requires financial institutions to implement a written information security program that is appropriate to the entity's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its program, each financial institution must also: (1) assign one or more employees to oversee the program; (2) conduct a risk assessment; (3) put safeguards in place to control the risks identified in the assessment and regularly test and monitor them; (4) require service providers, by written contract, to protect customers' personal information; and, (5) periodically update its security program.

GLB regulations require entities to prepare a written information security plan that describes an entity's program to protect client information. All programs must be appropriate to the size and complexity of the entity, the nature and scope of its activities, and the sensitivity of the client information at issue.

Entities significantly engaged in financial activities must:

1. Designate an employee or employees to coordinate the safeguards.
2. Identify and assess the risks to customer information in each relevant area of an entity's operation and evaluate the effectiveness of current safeguards for controlling these risks.
3. Design a safeguards program and implement detailed plans to regularly monitor it.
4. Select appropriate service providers, require them (by contract) to implement the safeguards, and oversee them.
5. Evaluate the program and explain adjustments in light of changes to an entity's business arrangements or the results of security tests or monitoring.

The Act states that the Safeguards Rule remains with the FTC and the prudential banking regulator, which could include the CFPB for appropriately qualifying financial institutions.

A companion to the Safeguards Rule, the FTC's Disposal Rule, has been the subject of recent enforcement. The Disposal Rule requires that companies dispose of credit reports and information derived from them in a safe and secure

manner. In November 2012, the FTC settled a matter involving the disposal of consumer information into trash dumpsters, and it assessed significant civil penalties. Considering the CFPB's stated focus on financial institutions' liability for service provider activities, it is important to verify compliance with the Disposal Rule for both financial institutions and any service providers.

On August 29, 2016, the FTC announced that it is opening a public comment period to evaluate the Safeguards Rule. The FTC is seeking comment on the economic impact and benefit of the Safeguards Rule as well as whether state and local laws conflict with the rule. The agency also wants to analyze whether technological, economic, or industry changes have affected the rule. The public comment period will run until November 7, 2016.

Implications/Best Practices:

None. State entities do not fall under the definition of "financial institution" under GLB. Nevertheless, as a matter of creating policies for "best practices," it may be useful to consider the following implications that apply to "financial institutions":

Financial institutions should:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems.
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.
- Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

Additionally, financial institutions should develop a written information security system, develop a written response program, and develop procedures for:

- Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information breaches have occurred.
- Notifying its primary Federal regulator (if applicable) as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information.
- Immediately notifying law enforcement in situations involving likely criminal violations requiring immediate attention.
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access, such as by monitoring, freezing, or closing affected accounts, while preserving records and other evidence.
- Disposing of customer information in a secure manner and, where applicable, in a manner consistent with the FTC's Disposal Rule.
- Developing policies for employees who telecommute or those who store or access customer information from their personal computers or mobile devices.

Sources:

FTC – Gramm-Leach-Bliley Act Legal Resources
http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act

16 C.F.R. Part 313 – Privacy of Consumer Financial Information
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr;sid=1e9a81d52a0904d70a046d0675d613b0;rgn=div5;view=text;node=16%3A1.0.1.3.37;idno=16;cc=ecfr

16 C.F.R. Part 314 – Standards for Safeguarding Customer Information
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title16/16cfr314_main_02.tpl

FTC , Bureau of Consumer Protection, Division of Financial Practices – Gramm-Leach-Bliley Act, Privacy of Consumer Financial Information
https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

FTC, Bureau of Consumer Protection – Disposing of Consumer Report Information? New Rule Tells How
http://www.business.ftc.gov/documents/alt152-disposing-consumer-report-information-rule-tells-how

Principles:

Accountability, Security Safeguards, Notice

1.9. Fair Credit Reporting Act as amended (FCRA) (including the Fair and Accurate Credit Transactions Act of 2003 (FACT Act))

15 U.S.C. § 1681 *et seq*.; 16 C.F.R. § 682; 72 Fed. Reg. 63718 *et seq*. (Nov. 9, 2007)

Description:

The Fair Credit Reporting Act (FCRA), Public Law 108-159, December 4, 2003, governs a consumer reporting agency's creation and disclosure of consumer reports. A consumer reporting agency is "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." This summary will not address the consumer reporting agency's responsibilities or the responsibilities of furnishers of information to consumer reporting agencies.

Entities procuring consumer reports must comply with FCRA. A consumer report concerns a "consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" and may be used for credit, insurance, employment, or other business decision making. In the employment context, notice must be given that a consumer report will be procured and authorization obtained. Before an adverse action is taken, the person intending to take the action must provide the consumer with notice, a copy of the report, including the disclosure of the person's credit score and related information, and a description of their rights. In an employee misconduct investigation conducted by a third party, notice does not need to be given to the employee, and no authorization is required. At the end of the investigation, the employee is only entitled to a notice of adverse action and a summary of the report. Consumer reports may only be used for authorized purposes; however, a consumer's identifying information may be given to a governmental agency without regard to the purpose. Before an entity procures an investigative consumer report, which is a report based upon personal interviews with neighbors, friends, or associates, it must give notice to the consumer and certify compliance to the consumer reporting agency. FCRA generally requires that consumers be given notice and an opportunity to opt-out with respect to marketing from organizations affiliated with the original receiver of the consumer report.

FCRA also governs truncation of credit card and debit card numbers. Machines that print receipts for credit card or debit card transactions shall not print more than the last 5 digits of the card number or the expiration date.

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Public Law 111–203 (July 21, 2010) also impacted FCRA and FACT Act. Primary rulemaking authority was transferred to the Consumer Financial Protection Bureau (CFPB), which impacted prior interpretations and commentary on FCRA. On July 26, 2011, the FTC rescinded its Statements of General Policy or Interpretation

("Commentary") under the FCRA, which were initially issued in 1990. The FTC stated that the Commentary was "obsolete" and "stale" due to its age and the number of revisions and amendments to FCRA since 1990. Since the "Commentary" was rescinded, it was not transferred to the CFPB and is no longer guiding or relevant in interpreting FCRA.

Enforcement actions may be brought by the FTC, SEC, and CFPB. There are civil and criminal penalties.

Effective January 1, 2013, employers that use credit reports as part of the background screening in their hiring process must use a new FCRA notice. The CFPB issued regulations updating the notice entitled "A Summary of Your Rights Under the FCRA," among other notices. The primary change involves making the CFPB, not the FTC, the point of contact for questions pertaining to the FCRA. The CFPB does not supervise background checks, but it exercises rulemaking and enforcement over the FCRA. In fact, the CFPB is specifically excluded from jurisdiction over consumer reports that are not used in connection with the offering of consumer financial products or services, such as used for tenant screening, employment, etc.

On February 7, 2012, the FTC warned marketers of six mobile background screening apps that they may be in violation of FCRA. The letter states "If you believe your background reports are being used for FCRA or other FCRA purposes, you and your customers who are using your reports for such purposes must comply with FCRA…." The FTC also stated that it had made no determination whether the companies are violating the FCRA, but encouraged them to review their apps and their policies and procedures to be sure they comply with the FCRA.

The FCRA has been upheld as constitutional with respect to its limitations on the length of time information may be reported. On May 3, 2012, the FTC, the CFPB, and the Department of Justice filed a memorandum of brief supporting the constitutionality of FCRA in *King v. General Information Services Inc*. (GIS), 903 F. Supp.2d 303 (E.D. Pa. 2012). GIS argued that FCRA is an unconstitutional restriction of free speech citing the recent Supreme Court decision in *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011), but the federal court concluded that the FCRA directly advances a government interest, balances the needs of businesses to perform background checks, and ensures consumer privacy.

On May 19, 2016, a bill (H.R. 5282) was introduced to amend the FCRA. The proposed reforms include a ban on the use of credit information in most employment decisions and a requirement that lenders provide consumers with copies of any reports used for underwriting prior to a loan agreement.

Note:

The FACT Act added several sections to FCRA, primarily of interest to banking institutions and consumer reporting agencies but also potentially pertinent to any entity that maintains consumer information or is a creditor. Regulations have now been issued which provide further compliance details. The FACT Act amends FCRA by requiring that any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of any such information or compilation. One purpose of the FACT Act is to reduce the risk of consumer fraud and related harms, including identity theft, created by improper disposal of consumer information.

Any business, regardless of industry, that obtains a consumer report or information derived from a consumer report will be subject to the record disposal rule imposed by section 215(a) of the FACT Act. This includes entities that possess or maintain consumer information for a business purpose such as landlords, government agencies, utility companies, telecommunication companies, employers, and other users of consumer reports.

Any person that maintains or possesses consumer information is required to take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. Entities covered by the FACT Act will need to consider the sensitivity of the consumer information, the nature and size of the entity operations, the costs and benefits of different disposal methods, and relevant technological changes. The FTC considers "reasonable measures" to include establishment of policies and procedures for disposal, as well as proper employee training. To this end, the FACT Act and its implementing regulations also curtail the use and sharing of consumer reports among affiliated entities.

Numerous provisions of the FACT Act significantly limit the State's ability to regulate much of FCRA's subject matter, as amended, including the ability of states to adopt stronger laws. Specific provisions in the FACT Act highlight areas of exclusive federal regulation and state law preemption.

Like most of the other consumer oriented federal laws, the CFPB will be responsible for issuing rules under the FACT Act.

See Section 1.9.1 for a detailed discussion on the Red Flags Rule.

Implications:

- Departments shall assess where they procure consumer reports.
- Division of Personnel and State Departments, as appropriate, shall adopt policies and procedures to ensure that consumer reports are properly procured and properly destroyed.
- The Chief Privacy Officer shall forward the information regarding the FACTA disposal requirements to the Director of Information Security.

- Division of Purchasing and Departments shall adopt policies and procedures to ensure that all machines purchased that print credit card and debit card receipts shall not print more than the last 5 digits of the card or the expiration date.
- Departments shall periodically assess whether they are subject to the Red Flag Rules.
- Departments that are subject to the Red Flag rules will develop written programs to detect, prevent, and mitigate identity theft in connection with covered accounts.

Sources:

15 U.S.C. § 1681 *et seq.* – Credit Reporting Agencies
http://www.law.cornell.edu/uscode/text/15/chapter-41/subchapter-III

Consumer Protection Financial Bureau – Supervision and Examination Manual
http://www.consumerfinance.gov/guidance/supervision/manual/

12 C.F.R. Part 1022 – Fair Credit Reporting (Regulation V)
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title12/12cfr1022_main_02.tpl

H.R. 5282 – Comprehensive Consumer Credit Reporting Reform Act of 2016
https://www.congress.gov/bill/114th-congress/house-bill/5282

Principles:

Notice, Consent, Minimum Necessary and Limited Use, Security Safeguards

1.9.1. Identity Theft "Red Flags" Rule

16 C.F.R. § 681.1

Description:

The Identity Theft "Red Flags" Rule (the Rule) requires "creditors" and "financial institutions" to develop written plans to prevent and detect identity theft. "Creditors" and "financial institutions" are broadly defined in the Rule. The Dodd-Frank Act added swap dealers and major swap participants to those entities that must comply with identity red flag rules and guidelines. The Rule is a section of the Fair and Accurate Credit Transactions Act (FACT Act) of 2003, a federal law which requires the establishment of guidelines for financial institutions and creditors regarding identity theft. The Rule sets out how certain businesses and organizations must develop, implement, and administer their own identity theft prevention programs. Each program must include four basic elements, which together create a framework to address the threat of identity theft:

1) Each program must include reasonable policies and procedures to identify the "red flags" of identity theft that may occur in the day-to-day operation of a business. Red flags are suspicious patterns, practices, or specific activities that indicate the possibility of identity theft. For example, if a customer has to provide some form of identification to open an account, an ID that looks fake would be a "red flag."

2) Each program must be designed to detect the red flags previously identified. For example, if a fake ID is identified as a red flag, there must be procedures in place to detect possible fake, forged, or altered identification.

3) Each program must spell out appropriate actions to take when red flags have been detected.

4) Because identity theft is an ever-changing threat, each program must address periodical re-evaluations of the red-flag program procedures.

Initially, the FTC took the position that the Rule was applicable to all entities that regularly permit deferred payments for goods or services (i.e. attorneys and medical providers who bill their clients after services are rendered). However, this position was overruled by Congress when the Red Flag Program and Clarification Act of 2010 was signed by President Obama on December 18, 2010. The Act amended the definition of "creditor" under the Rule to only apply to those who not only regularly extend, renew, or continue credit, but also regularly and in the ordinary course of their business, (i) obtain or use consumer reports, directly or indirectly, in connection with the transaction; (ii) furnish information to consumer reporting agencies, in connection with a credit transaction; or (iii) advance funds

to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person. In addition, the amendment limited the definition of "creditor" to exclude those "that advance funds on behalf of a person for expenses incidental to a service provided to that individual." These amendments exclude most attorneys and medical providers from the Rule, but the Rule would still be applicable to those that obtain or use consumer reports or report to consumer reporting agencies.

On May 29, 2014, the Federal Reserve System cemented these changes by issuing a final rule Regulation V. This final rule amended the definition of "creditor" in the Red Flags rule to include only the Clarification Act's definition. While the rule limits the definition of 'creditor' to exclude certain groups from compliance with the Red Flag Rules, the Rules still apply to all financial institutions.

On October 28, 2015, the Federal Deposit Insurance Corporation ("FDIC") adopted an amendment to its regulations. That amendment added "state savings association" to the scope of the regulations and brought the definition of "creditor" into conformity with the Clarification Act. Finally, the FDIC rescinded and removed rule writing authority previously transferred to CFPB. A separate amendment issued by the FDIC on the same day consolidated redundant rules from the now defunct Office of Supervision into part 364.

In April 2013, the Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC") issued joint final rules and guidelines to require certain regulated entities to establish programs to address risks of identity theft. The final rules set forth provisions requiring the entities under the jurisdiction of the SEC and CFTC 1) to address identity theft by requiring financial institutions and creditors to develop and implement a written identity theft prevention program to detect, prevent and mitigate identity theft in connection with existing or the opening of new accounts; and 2) to establish special requirements for any credit and debit card issuers that are subject to the commissions' jurisdictions to assess their rules. Generally, these rules do not contain new requirements that are different from the FTC rules, nor do they expand the scope of those rules. The rules and guidelines do, however, include examples and minor language changes to help securities and commodities firms comply.

Implications

- Departments shall periodically assess whether they are subject to the Red Flags Rule.
- Departments shall identify red flags for its own type of covered accounts and incorporate them into the Department's identity theft program.
- Departments that are subject to the Red Flags Rule will develop written programs to detect, prevent and mitigate identity theft in connection with covered accounts.
- Departments may want to consider incorporating the FTC's "illustrative examples" to the extent applicable into its identity theft program.

- Though normally excluded from the Red Flags Rule as a result of the Red Flag Program and Clarification Act, hospitals and medical providers should examine their usage of credit reports or their reporting to credit agencies so as to be or remain excluded from the Rule.

Sources:

Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule:
Department of the Treasury, Office of the Comptroller of the Currency, 12 C.F.R. Part 41 – Fair Credit Reporting
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=f0fbbb92bffbadf769c31ebca6c51f68&tpl=/ecfrbrowse/Title12/12cfr41_main_02.tpl

Federal Reserve System, 12 C.F.R. Part 222 – Fair Credit Reporting (Regulation V)
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=f0fbbb92bffbadf769c31ebca6c51f68&tpl=/ecfrbrowse/Title12/12cfr222_main_02.tpl

FDIC, 12 C.F.R. Parts 334 – Fair Credit Reporting
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=f0fbbb92bffbadf769c31ebca6c51f68&rgn=div5&view=text&node=12:5.0.1.2.23&idno=12

FDIC, Final Rule, 80 Fed. Reg. 65913 – Removal of Transferred OTS Regulations Regarding Fair Credit Reporting and Amendments; etc.
https://www.regulations.gov/document?D=FDIC-2015-0152-0001

FDIC, 12 C.F.R. Parts 364 – Standards for Safety and Soundness
http://www.ecfr.gov/cgi-bin/text-idx?SID=8731ad36153c57f09853b641cca8ef18&mc=true&tpl=/ecfrbrowse/Title12/12cfr364_main_02.tpl

FDIC, Final Rule, 80 Fed. Reg. 65903 – Removal of Transferred OTS Regulations Regarding Safety and Soundness Guidelines and Compliance Procedures; Rules on Safety and Soundness,
https://www.regulations.gov/document?D=FDIC-2015-0155-0001

National Credit Union Administration, 12 C.F.R. Part 717 – Fair Credit Reporting
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=f0fbbb92bffbadf769c31ebca6c51f68&rgn=div5&view=text&node=12:7.0.2.3.19&idno=12

FTC, 16 C.F.R. Part 681 – Identity Theft Rules
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title16/16cfr681_main_02.tpl

Commodity Futures Trading Commission, 17 C.F.R. Part 162 – Protection of Consumer Information Under the Fair Credit Reporting Act
http://www.ecfr.gov/cgi-bin/text-idx?SID=4ba6f4d9a816d352d161de2375cd9e7b&node=17:2.0.1.1.27&rgn=div5

SEC, 17 C.F.R. Part 248 – Regulations S-P, S-AM, AND S-ID
http://www.ecfr.gov/cgi-bin/text-idx?SID=ef1578169814731302470d13e7c7563a&mc=true&tpl=/ecfrbrowse/Title17/17cfr248_main_02.tpl

FTC, Bureau of Consumer Protection – Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business
http://www.business.ftc.gov/documents/bus23-fighting-identity-theft-red-flags-rule-how-guide-business

American Bar Ass'n v. FTC, 636 F.3d 641 (D.C. Cir. 2011)
https://www.courtlistener.com/cadc/24ev/american-bar-assn-v-ftc/

Principles:
Notice, Consent, Minimum Necessary and Limited Use, Security Safeguards

1.10. Family Educational Rights and Privacy Act of 1974 (FERPA)

20 U.S.C. § 1232g; 34 C.F.R. Part 99

Description:

The Family Educational Rights and Privacy Act of 1974 (FERPA) protects the privacy of student education records and applies to any public or private agency or institution (may be referred to as school) that receives funds under an applicable program of the U.S. Department of Education. Education records are those records, files, documents, and other materials which contain information directly related to a student and are maintained by an educational agency or institution. There are a number of exempted categories of records.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are “eligible students.”

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school; parents must be granted access within 45 days after the request is made. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record to a third-party. The authorization form may be paper or electronic. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions:
    - School officials with legitimate educational interest;
    - Other schools to which a student is transferring;
    - Specified officials for audit or evaluation purposes;
    - Appropriate parties in connection with financial aid to a student;
    - Organizations conducting certain studies for or on behalf of the school;
    - Accrediting organizations;
    - To comply with a judicial order or lawfully issued subpoena;
    - Appropriate officials in cases of health and safety emergencies; and,
    - State and local authorities, within a juvenile justice system, pursuant to specific state law.

Schools may disclose, without consent, “directory” information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them.

Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter or inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

Failure to comply with FERPA can result in loss of funds from any of the U.S. Department of Education’s applicable programs.

Regulations for FERPA are codified in 34 C.F.R. Part 99. Effective January 3, 2012, the regulations were amended to provide additional rules regarding use of personally identifiable information (PII). For example, the regulations were amended to clarify that a FERPA-permitted entity from which the PII originated is responsible for using reasonable methods to ensure to the greatest extent practicable that any entity designated as its authorized representative complies with FERPA requirements. FERPA-permitted entities are required to use written agreements to designate and authorize a representative (other than an employee) who is allowed to access PII from educational records without prior written consent in connection with any audit, evaluation, or enforcement or compliance activity. The written agreement must do the following:

- Specify how the work falls within the exception of Section 99.31(a)(3), including a description of the PII from educational records that will be disclosed and how the PII from educational records will be used, and
- Include policies and procedures to protect PII from further disclosure, including limitation of the use of PII to authorized representatives with legitimate interests in the audit, evaluation, or enforcement or compliance activity.

Implications:

- Departments must assess whether they collect or maintain student education records and receive funds under an applicable program of the U.S. Department of Education to determine FERPA coverage.
- If FERPA applies, Departments shall adopt policies and procedures to ensure that the various requirements are in place.
- *See* Section 3.22 for a summary of the W. Va. Student Data Accessibility, Transparency, and Accountability Act.

Sources:

20 U.S.C. § 1232g – Family Educational and Privacy Rights
http://www.law.cornell.edu/uscode/text/20/1232g

34 C.F.R. Part 99 – Family Educational Rights and Privacy
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=f4adaebd92dd4c26533daf9af0f02aba&rgn=div5&view=text&node=34:1.1.1.1.33&idno=34

Principles:

Notice, Consent, Individual Rights

1.11. Driver's Privacy Protection Act

18 U.S.C. §§ 2721-25

Description:

The Driver's Privacy Protection Act of 1994 (DPPA), 18 U.S.C. §§ 2721-25 restricts public disclosure of personal information contained in Department of Motor Vehicle (DMV) records. Personal information includes: the individual's photograph, social security number, driver's license number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information. Personal information does not include information on vehicular accidents, driving violations, and driver's status. DPPA applies to state DMVs and recipients of personal information from the DMV. DPPA permits the release of information to recipients who are using it for one or more specific statutory purposes, or where the subject of the record was furnished an opportunity to limit the release of the information and did not do so. The Act penalizes the procurement of information from motor vehicle records for an unlawful purpose or the making of a false representation to obtain such information from a DMV.

There are civil and criminal penalties for violation of this law. Additionally, there is a private right of action.

Implications:

- The DMV must have policies and procedures to ensure that personal information obtained in connection with the motor vehicle record is only used and disclosed as authorized by law or with the consent of the individual.
- Departments must assess whether they obtain personal information from the DMV.
- Departments obtaining personal information from DMV must ensure that they have policies and procedures detailing the use and disclosure of the personal information, as well as the record keeping requirements.
- *See* Section 3.10 for W. Va. Uniform Motor Vehicle Records Disclosure Act.

Source:

18 U.S.C. § 2721 – Prohibition on release and use of certain personal information from State motor vehicle records
http://www.law.cornell.edu/uscode/text/18/2721

18 U.S.C. § 2722 – Additional unlawful acts
http://www.law.cornell.edu/uscode/text/18/2722

18 U.S.C. § 2723 – Penalties
http://www.law.cornell.edu/uscode/text/18/2723

18 U.S.C. § 2724 – Civil action
http://www.law.cornell.edu/uscode/text/18/2724

18 U.S.C. § 2725 – Definitions
http://www.law.cornell.edu/uscode/text/18/2725

Principles:
Consent, Minimum Necessary and Limited Use, Security Safeguards

1.12. Telephone Consumer Protection Act, Telemarketing Sales Rules
47 U.S.C. § 227, 16 C.F.R. Part 310

Description:
The Telephone Consumer Protection Act, 47 U.S.C. § 227, requires entities who use the telephone to solicit individuals to provide such individuals with the ability to prevent future telephone solicitations. Those who engage in telephone solicitations must maintain and honor lists of individuals who request not to receive such solicitations for ten years. The Act prohibits unsolicited commercial telephone calls using an artificial or pre-recorded voice without consumer consent unless such a call is made to collect a debt owed to or guaranteed by the United States. It also prohibits the sending of unsolicited advertisements to facsimile machines.

The Telemarketing Sales Rule, 16 C.F.R. Part 310, regulates telemarketing with regard to deceptive and abusive telemarketing acts or practices. Significantly, this rule establishes the Federal Trade Commission's (FTC) Do-Not-Call list.

The FTC finalized an amendment to the Telemarketing Sales Rule on December 14, 2015. The changes (1) prohibit the use of certain abusive payment methods; (2) expand the prohibition against advance fee recovery services to include recovery for any previous transaction instead of only telemarketing transactions; and (3) clarify existing requirements relating to the Do-Not-Call list and verification of purchase.

The FTC has jurisdiction to enforce this rule against the private sector. The Federal Communications Commission (FCC) (with regard to interstate and international communications), State attorneys general, and private citizens may bring actions under these provisions against state government. State telemarketing laws are not preempted. *See* the discussion regarding Consumer Credit and Protection Act, Telemarketing, W. Va. Code § 46A-6F-601.
The FCC approved changes to its telemarketing rule on February 15, 2012, to further protect consumers from unwanted autodialed or prerecorded telephone calls often referred to as "robocalls." These rules took effect on July 11, 2012. They do the following:

- Require telemarketers to obtain prior express written consent from consumers, including by electronic means such as a website form, before placing a robocall to a consumer;
- Eliminate the "established business relationship" exemption to the requirement that telemarketing robocalls to residential wireline phones occur only with the prior express consent from the consumer;
- Require telemarketers to provide an automated, interactive "opt-out" mechanism during each robocall so that the consumer can immediately tell the telemarketer to stop calling; and
- Strictly limit the number of abandoned or "dead air" calls that telemarketers can make within each calling campaign.

On July 10, 2015, the FCC issued an Omnibus Order that closed certain loopholes in its robocall restrictions, including placing limits on calls to reassigned numbers. The Order also clarified that text messages are "calls" subject to the TCPA. In addition, consumers may revoke consent at-will. Finally, the Order waived the 2012 "prior express written consent" rule on a limited basis and exempted certain free, pro-consumer financial- and healthcare-related messages from the consumer consent requirement.

Implications:

- Departments must assess whether they engage in telemarketing.
- Departments that engage in telemarketing shall adopt policies and procedures to ensure compliance with this rule and W. Va. Code § 46A-6F-601.

Source:

47 U.S.C. § 227 – Restrictions on use of telephone equipment
http://www.law.cornell.edu/uscode/text/47/227

16 C.F.R. Part 310 – Telemarketing Sales
http://www.law.cornell.edu/cfr/text/16/310

47 C.F.R. §§ 64.1200-02 –Restrictions on Telemarketing, Telephone Solicitation, and Facsimile Advertising
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=679761cb47017786ce060d725840c27e&rgn=div6&view=text&node=47:3.0.1.1.11.12&idno=47

TCPA Omnibus Declaratory Ruling and Order
https://www.fcc.gov/document/tcpa-omnibus-declaratory-ruling-and-order

W. Va. Code § 46A-6F-601 – Abusive acts or practices
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=46a&art=6F&section=601#06F

FCC , Consumer Guide – Robocallshttp://transition.fcc.gov/cgb/consumerfacts/robocalls.pdf

FCC Consumer Guide – Stop Unwanted Calls, Texts, and Faxes
https://www.fcc.gov/stop-unwanted-calls

FCC Consumer Guide - Unwanted Telephone Marketing Calls
http://transition.fcc.gov/cgb/consumerfacts/tcpa.pdf

Complaint form
https://consumercomplaints.fcc.gov/hc/en-us

Principles:

Notice, Consent, Minimum Necessary and Limited Use, Security Safeguards

Note:

There are special marketing rules which do not neatly fit within the defined principles.

1.13. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, (CAN-SPAM Act)

15 U.S.C. §§ 7701-13

Description:

The CAN-SPAM Act establishes requirements for those who send commercial e-mail, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask e-mailers to stop spamming them.

The law covers e-mail whose primary purpose is advertising or promoting a commercial product or service, including content on a Website. The main provisions include the following:

- A ban on false or misleading header information (an e-mail's "From," "To," and routing information – including the originating domain name and e-mail address – must be accurate and identify the person who initiated the e-mail);
- A prohibition on deceptive subject lines;
- The requirement that e-mails give recipients an opt-out method (the sender has 10 business days to stop sending e-mail to the requestor's e-mail address); and
- The requirement that commercial e-mail be identified as an advertisement and include the sender's valid physical postal address.

The Federal Trade Commission (FTC) is authorized to enforce the CAN-SPAM Act against the private sector. CAN-SPAM also gives the Department of Justice the authority to enforce its criminal sanctions. Other federal and state agencies, such as the Attorney General, can enforce the law against organizations under their jurisdiction. Companies that provide internet access may sue violators as well.

Implications:

- Departments must assess whether they are sending commercial e-mail to advertise a product or service.
- Departments transmitting commercial e-mail to advertise or promote a product or service shall adopt policies and procedures to ensure compliance with this law.

Sources:

15 U.S.C. §§ 7701-13 – Controlling the Assault of Non-Solicited Pornography and Marketing
http://www.law.cornell.edu/uscode/text/15/7701

CAN-SPAM Act: A Compliance Guide for Business
http://business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business

16 C.F.R. Part 316 – CAN-SPAM Rule
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title16/16cfr316_main_02.tpl

Principles:
Notice, Consent

1.14. Junk Fax Prevention Act of 2005

47 U.S.C. § 227
47 C.F.R. §§ 64.201, 64.1200-02

Description:

The Junk Fax Protection Act of 2005, Public Law 109-21, 47 U.S.C. § 227, amends the Communications Act of 1934 to prohibit a person from using any telephone facsimile (fax) machine, computer, or other device to send to another fax machine, an unsolicited advertisement to a person who has requested that the sender not send such advertisements, or to any other person unless:

- the sender has an established business relationship with the person;
- the sender obtained the fax number through voluntary communication from the recipient or from an Internet directory or site to which the recipient voluntarily made the fax number available for public distribution; and
- the advertisement contains a conspicuous notice on its first page that the recipient may request not to be sent any further unsolicited advertisements and includes a domestic telephone and fax number (neither of which can be a pay-per-call number) for sending such a request.

Additionally, the Federal Communications Commission (FCC) has issued rules, 47 C.F.R. Part 64, regarding faxing advertisements; the fax must identify the sender on either the top or bottom margin of each page with the telephone number and the date and time the fax is sent.

The FCC (with regard to interstate and international communications) and the West Virginia Attorney General may enforce this law. There are civil and criminal penalties. Additionally, there is a private right of action.

Implications:

- Departments must assess whether they advertise by fax.
- Departments which advertise via fax shall ensure that they adopt policies and procedures in compliance with this law.

Sources:

Pub. L. No. 109-21 (July 9, 2009)
Junk Fax Prevention Act of 2005

47 U.S.C. § 227 – Restrictions on use of telephone equipment
http://www.law.cornell.edu/uscode/text/47/227

FCC Consumer Guide – Stop Unwanted Calls, Texts, and Faxes
https://www.fcc.gov/stop-unwanted-calls

FCC Consumer Guide – Junk Faxes

http://transition.fcc.gov/cgb/consumerfacts/unwantedfaxes.pdf

47 C.F.R. § 64.201 –Restrictions on Indecent Telephone Message Services
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=a1b9379cbfdf039a4414e25333142146&rgn=div6&view=text&node=47:3.0.1.1.11.2&idno=47

47 C.F.R. §§ 64.1200-02 – Restrictions on Telemarketing, Telephone Solicitation, and Facsimile Advertising
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=a1b9379cbfdf039a4414e25333142146&rgn=div6&view=text&node=47:3.0.1.1.11.12&idno=47

Principles:
Notice, Consent

1.15. Children's On-line Privacy Protection Act (COPPA)

15 U.S.C. § 6501 *et seq*., 16 C.F.R. Part 312

Description:

The Children's Online Privacy Protection Act of 1998 (COPPA), Public Law 105-277, 15 U.S.C. § 6501 *et seq*., which took effect in April of 2000, prohibits certain unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personal information from children on the Internet. The Federal Trade Commission (FTC) issued the Children's Online Privacy Protection Rule (the COPPA Rule) which imposes requirements on website or online services directed to children under 13 years of age or that have actual knowledge that they collect personal information from children under 13 years of age. This includes websites that allow children to use interactive communication tools. Therefore, even if a site is not collecting information about children, if a child's personal information can be made public on the site (such as through a message board), there may be COPPA liability.

Websites cannot require a child to provide personal information as a condition of participating when it is not necessary to do so.

The FTC oversees the implementation of this law, and its website provides extensive information on COPPA. With certain exceptions, COPPA is to be enforced by the FTC under the FTC Act. The FTC may enforce the state's compliance with COPPA or those acting under color of state law pursuant to the enforcement provisions of COPPA, which incorporate by reference the means, jurisdiction, powers, and duties of the FTC Act. Although such an instance may be rare, it is important for websites and online service providers to be cognizant of their online activities.

The State Attorney General may bring an action as *parens patriae* if he/she has reason to believe that an interest of the residents of West Virginia has been or is threatened or adversely affected by the engagement of any person in a practice that violates any regulation of COPPA. The Attorney General may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction. Suits may be brought to achieve compliance with the Act and to recover monetary damages.

The FCC amended the COPPA Rule effective July 1, 2013, to clarify its scope and strengthen its protections for children's personal information in light of changes in online technology since the Rule went into effect in April 2000. The final amended Rule includes modifications to the definitions of operator, personal information, and Web site or online service directed to children. The amended Rule also updates the requirements set forth in the notice, parental consent, confidentiality and security, and safe harbor provisions and adds a new provision addressing data retention and deletion. Additionally, the final amendments:

a. Modify the list of “personal information” that cannot be collected without parental notice and consent, clarifying that this category includes geolocation information, photographs, and videos;

b. Offer companies a streamlined, voluntary, and transparent approval process for new ways of getting parental consent;

c. Close a loophole that allowed kid-directed apps and websites to permit third parties to collect personal information from children through plug-ins without parental notice and consent;

d. Extend coverage in some of those cases so that the third parties doing the additional collection also have to comply with COPPA;

e. Extend the COPPA Rule to cover persistent identifiers that can recognize users over time and across different websites or online services, such as IP addresses and mobile device IDs;

f. Strengthen data security protections by requiring that covered website operators and online service providers take reasonable steps to release children’s personal information only to companies that are capable of keeping it secure and confidential;

g. Require that covered website operators adopt reasonable procedures for data retention and deletion; and

h. Strengthen the FTC’s oversight of self-regulatory safe harbor programs.

In November 2015, the FTC approved a new method for companies to get parents’ consent for their children to access online services covered by COPPA. The FTC approved the use of “Face Match to Verified Photo Identification” as a method to verify that the person providing consent for a child to use an online service is in fact the child’s parent.

Implications:

COPPA requires that websites and online services directed to children under age 13 must:

- Post a clearly written privacy policy with links to the notice provided on the home page and at each area where the site or online service collects personal information from children.
- Describe the kinds of information collected from children, (i.e. name, address, e-mail, hobbies, age [this applies to all information, not just personal information]).
- Explain how the information is collected, whether directly from the child and/or behind the scenes through cookies.

- Explain how the website operator uses the personal information (i.e. marketing to children, notifying contest members, etc.), and whether it is disclosed to third parties.
- Provide parents with contact information, address, phone number, and e-mail address, for all operators collecting or maintaining children's personal information.
- Obtain parental consent before collecting, using, or disclosing personal information about a child.
- Provide parents with the ability to review, correct, and delete information about their children collected by such services.
- Maintain reasonable procedures "to protect the confidentiality, security, and integrity of personal information collected from children."

Source:

15 U.S.C. Chapter 91 – Children's Online Privacy Protection Act
http://www.law.cornell.edu/uscode/text/15/chapter-91

16 C.F.R. Part 312 – Children's Online Privacy Protection Rule
http://www.law.cornell.edu/cfr/text/16/312

Jest8 Limited Trading as Riyo's Application for Approval of a Verifiable Consent Method
https://www.ftc.gov/system/files/attachments/press-releases/ftc-seeks-public-comment-riyo-proposal-parental-verification-method-under-coppa-rule/150731riyoapplication.pdf

80 Fed. Reg. 47429 – FTC Request for Public Comment on Proposed Parental Consent Method
https://www.ftc.gov/system/files/documents/federal_register_notices/2015/08/150807riyocoppafrn.pdf

Complying with COPPA: Frequently Asked Questions (revised March 2015)
http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions

Principles:

Notice, Minimum Necessary and Limited Use, Consent, Security Safeguards

1.16. Cable Communications Policy Act (CCPA)

47 U.S.C. § 551

Description:

The Cable Communications Policy Act of 1984, 47 U.S.C. § 551, protects the personal customer information held by cable service providers. Pursuant to the CCPA, cable service providers must obtain prior written or electronic consent from a subscriber before collecting any personal information. Consent is not required to obtain information "necessary to render cable services;" nor is it required for information used to detect unauthorized reception. Disclosure also generally requires prior consent, with the same two exceptions for business necessity and detection of cable piracy. Disclosure of personal information without consent is also permitted pursuant to a court order. The subscriber must be notified and offered an opportunity to appear and contest the order. Disclosures may not generally include information about the subscriber's particular selections of video programming.

A cable service provider must destroy personal information when it is no longer needed for the purposes for which it was collected (and there are no pending requests for access). It must take appropriate steps to prevent unauthorized access of customers' personal information for as long as it is held.

Any person may bring a civil action against a cable provider for violations of this section and may seek actual and punitive damages.

CCPA specifically includes such "other services" as "radio and wire communications," which likely would include providers of cable broadband Internet service. The provisions of the CCPA probably cannot be stretched to apply to direct broadcast satellite (DBS) service even though they provide functionally similar services.

In 2001, the USA-Patriot Act, Public Law 107-56, narrowed the Cable Act's privacy provisions, clarifying that companies who offer cable-based internet or telephone services will be subject to the requirements of the Cable Act to notify subscribers of government surveillance requests only when detailed cable viewing information is being sought. Otherwise, cable operators can respond to a government surveillance request under the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-22, which does not require service providers to notify subscribers of requests.

Implications:

Under the CCPA, Departments, and particularly colleges and universities who are or may be cable service providers, must provide a written notice of privacy practices to each subscriber (customer) at the time of entering into a service contract and at least once a year thereafter. The privacy notice must specify:

- The nature of the personally identifiable information that is or may be collected, and the uses to which it may be put.
- The “nature, frequency, and purpose” of any disclosure that may be made of such information, including identification of the persons to whom those disclosures may be made.
- How long the information may be maintained by the cable service provider.
- Where and how the subscriber may have access to the information about himself or herself.
- The subscriber's right to bring legal action if the requirements of the law are not followed.

Note:

States are not preempted from enacting laws which provide greater privacy protections than the CCPA.

Sources:

47 U.S.C. § 551 – Protection of subscriber privacy
http://www.law.cornell.edu/uscode/text/47/551

18 U.S.C. §§ 2510-22 – Electronic Communications Privacy Act of 1986
-
http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119

Principles:

Security Safeguards, Consent, Notice, Individual Rights, Minimum Necessary and Limited Use

1.17. Video Privacy Protection Act

18 U.S.C. § 2710

Description:

The Video Privacy Protection Act of 1988 (VPPA), 18 U.S.C. § 2710, as originally passed, created one of the strongest consumer privacy protection laws prohibiting disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual material." The Act has several provisions, including:

- A general ban on the disclosure of personally identifiable rental information unless the consumer consents specifically and in writing.
- Disclosure to police officers only with a valid warrant or court order.
- Disclosure of "genre preferences" along with names and addresses for marketing, but allowing customers to opt out.
- Exclusion of evidence acquired in violation of the Act.
- A requirement that video stores destroy rental records no longer than one year after an account is terminated.

Issues remain about the applicability of the Act to other rental records, including DVDs and video games, which are commonly rented by the same stores that rent video cassettes. The plain language of the Act would indicate that it applies broadly to all such records, but no cases have interpreted the language. Since the passage of the U.S. Patriot Act, which expands law enforcement powers to permit use of administrative subpoena or otherwise procure information such as library records and individual purchasing records "in the course of an ongoing investigation" (a lower standard than the traditional warrant), it is unclear whether this Act's ban is circumvented by the use of administrative subpoena.

A person may sue for violations of VPPA, including actual damages (statutorily not less than $2,500.00), punitive damages, and attorney's fees.

The Video Privacy Protection Act Amendments Act of 2012, Public Law 112-258 (January 10, 2013), amended 18 U.S.C. § 2710(b)(2)(B) to allow a video tape service provider to disclose personally identifiable information concerning any consumer to any person with the informed, written consent (including through an electronic means using the Internet) of the consumer that (1) is in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer; (2) at the election of the consumer (a) is given at the time the disclosure is sought or (b) is given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner; and (3) the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election.

Implications:

- Departments that provide video cassette rental services should develop policies implementing the protections of the VPPA.
- Departments that are subpoenaed or otherwise contacted by federal enforcement authorities requesting the disclosure of VPPA, protected material should contact the Attorney General and the State Privacy Officer.

Source:

18 U.S.C. § 2710 – Wrongful disclosure of video tape rental or sale records
http://www.law.cornell.edu/uscode/text/18/2710

Pub. L. No. 112-258 (January 10, 2013)
http://www.gpo.gov/fdsys/pkg/PLAW-112publ258/html/PLAW-112publ258.htm

Principles:

Security Safeguards, Minimum Necessary and Limited Use

1.18. United States Patriot Act

50 U.S.C. § 1861; 18 U.S.C. § 2702

Description:

The United States Patriot Act, Public Law 107-56, with amendments ("the Act") was enacted to deter and punish terrorist acts in the United States and around the world. There are a number of provisions in the Act that relate to disclosure of information to the federal government in support of a variety of investigations. Two sections of the Act are discussed below.

50 U.S.C. § 1861 governs access to certain business records for foreign intelligence purposes and international terrorism investigations. According to the Act, the Director of the FBI or a designee may make an "application for an order requiring the production of tangible things for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." For each disclosure, "minimization procedures" are to be established, limiting the dissemination only to those individuals to whom disclosure is absolutely necessary. Tangible things can include library circulation records, library patron records, books sales records, customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person. The Patriot Act also requires credit reporting entities to furnish consumer reports to a government agency authorized to conduct counterterrorism investigations.

18 U.S.C. § 2702 governs voluntary disclosure of customer communications or records. Generally, the section states that an "entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." However, enactment of the Patriot Act created an exception to allow disclosure "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." The Attorney General must report the number of such voluntary disclosures to Congress.

Note:

In 2005, the USA Patriot and Terrorism Prevention Reauthorization Act of 2005, Public Law 109, 177 was passed.

In 2011, the Patriot Act was renewed by Congress. *See* Patriot Sunsets Extension Act of 2011, Public Law 112-14, signed May 16, 2011. The three provisions that were renewed by the Patriot Sunsets Extension Act of 2011 expired on June 1, 2015. On June 2, 2015, Congress passed the USA Freedom Act to take their place. The USA Freedom Act renewed a majority of the expired provisions, but ended the National Security Agency's practice of collecting bulk data about Americans' phone calls.

Implications:

- Departments are subject to the disclosure requirements or parameters identified in the Patriot Act. There is limited case law interpreting the Patriot Act and how it relates to state or federal privacy laws.
- Departments that are subpoenaed or otherwise contacted by federal enforcement authorities requesting the disclosure of otherwise protected material should contact their designated attorney and Privacy Officer.

Sources:

50 U.S.C. § 1861 – Access to certain business records for foreign intelligence and international terrorism investigations
http://www.law.cornell.edu/uscode/text/50/1861

18 U.S.C. § 2702 – Voluntary disclosure of customer communications or records
http://www.law.cornell.edu/uscode/text/18/2702

Principles:

Minimum Necessary and Limited Use

1.19. Computer Fraud and Abuse Act of 1986 (CFAA)

18 U.S.C. § 1030

Description:

The Computer Fraud and Abuse Act of 1986 (CFAA), Public Law 99-474 (October 16, 1986) is codified in 18 U.S.C. § 1030. The CFAA was intended to reduce "hacking" of computer systems. It applies to any "protected computer," which is any computer used in interstate or foreign commerce or communication by the federal government, a federally regulated financial institution, or any private computer system network spanning more than one state. CFAA provides for criminal and civil liability for accessing a protected computer without authorization and obtaining anything of value. If the only thing of value is the use of the computer, the value of such use must be greater than $5,000 during any one-year period.

The Act prohibits the following:

- To knowingly access a computer without authorization, or in excess of authorization, in order to obtain classified United States defense or foreign relations information with the intent to harm the United States or benefit a foreign nation.
- To obtain information, via unauthorized access, from the financial records of a financial institution or from any protected computer if the conduct involves interstate or foreign communication.
- To access a computer to use, destroy, modify, or disclose information found in a "federal interest" computer system, as well as to prevent authorized use of any computer used for government business if the usage interferes with government activities.
- To knowingly, and with the intent to defraud, participate in the trafficking of passwords or similar information through which computers can be accessed without authorization.

This law was amended in 1994, 1996, and in 2001 by the U.S. Patriot Act. The U.S. Patriot Act increased the scope and penalties of the CFAA by:

- Raising the maximum penalty for violations to 10 years (from 5) for a first offense and 20 years (from 10) for a second offense.
- Ensuring that violators only need to intend to cause damage generally, not intend to cause damage or other specified harm over the $5,000 statutory damage threshold.
- Allowing aggregation of damages to different computers over a year to reach the $5,000 threshold.
- Enhancing punishment for violations involving any (not just $5,000) damage to a government computer involved in criminal justice or the military.
- Including damage to foreign computers involved in U.S. interstate commerce.

- Including state law offenses as priors for sentencing.
- Expanding the definition of loss to expressly include time spent investigating and responding for damage assessment and for restoration.

The jurisdiction to investigate cases under this law is assigned jointly to the FBI and the U.S. Secret Service (USSS). The FBI is assigned to investigate cases involving espionage, misuse of classified data, government related fraud, terrorism, bank fraud, wire fraud, and organized crime. The USSS has been given oversight responsibility for investigations of federal interest crimes relating to a variety of offenses, including financial institution fraud and electronic crimes involving network intrusion where funds and data are stolen or manipulated.

Note:

This is parallel to the West Virginia Computer Crime and Abuse Act (*See* Section 3.12) governing misconduct in West Virginia. West Virginia's statute prohibits the modification, destruction, access to, duplication of, or possession of data, documentation, or computer programs without the consent of the owner. The disclosure of restricted access codes or other restricted information to unauthorized persons is prohibited, and generally the degree of punishment or the magnitude of the fine is based on the degree of damage or cost. There is no breach reporting requirement.

Implications:

- Departments must assess current computer privacy policies.
- Departments must implement and develop policies in light of West Virginia's computer crime law to prevent computer fraud and abuse.

Sources:

18 U.S.C. § 1030 – Fraud and related activity in connection with computers
http://www.law.cornell.edu/uscode/text/18/1030

US Justice Department, Computer Crime & Intellectual Property Section
http://www.justice.gov/criminal/cybercrime/reporting.html

Congressional Research Service Report RS20830 – Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws
(October 15, 2014)
http://www.fas.org/sgp/crs/misc/RS20830.pdf

Congressional Research Service Report 97-1025 – Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws (October 15, 2014)
http://www.fas.org/sgp/crs/misc/97-1025.pdf

W. Va. Code §§ 61-3C-1 to -21 – West Virginia Computer Crime and Abuse Act
http://www.legis.state.wv.us/wvcode/ChapterEntire.cfm?chap=61&art=3C

Principles:
Security Safeguards, Minimum Necessary and Limited Use, Consent

1.20. National Crime Prevention and Privacy Compact (NCPPC)

42 U.S.C. Chapter 140, Subchapter II, §§ 14611-16

Description:

The National Crime Prevention and Privacy Compact (NCPPC) creates an electronic information sharing system whereby the FBI and participating states can exchange criminal records for non-criminal justice purposes authorized by federal or state law, and it provides reciprocity among the states to share records in a uniform fashion without charging each other for information. The Compact became effective in 1999. States participate following ratification of the Compact. West Virginia ratified the compact in 2006. *See* W. Va. Code § 15-2-24a, *See also* Section 3.20.

Implications:

- The West Virginia authorized criminal record repository must make all unsealed criminal history records available in response to authorized, noncriminal justice requests.
- Records received from other states must be screened to delete any information not otherwise permitted to be shared under West Virginia law.
- Records produced to other states are governed by the NCPPC and not West Virginia state law.

Source:

42 U.S.C. Chapter 140, Subchapter II, §§ 14611-16 – Exchange of Criminal History Records for Noncriminal Justice Purposes
http://www.law.cornell.edu/uscode/text/42/chapter-140/subchapter-II

28 C.F.R. Chapter IX, Parts 901-907 – National Crime Prevention and Privacy Compact Council
http://www.law.cornell.edu/cfr/text/28/chapter-IX

U.S. Department of Justice, Office of Justice Programs – National Crime Prevention
and Privacy Compact: Resource Materials, NCJ 171671 (January 1998)
http://www.bjs.gov/content/pub/pdf/ncppcrm.pdf

W. Va. Code § 15-2-24a – National Crime Prevention and Privacy Compact
http://www.legis.state.wv.us/wvcode/ChapterEntire.cfm?chap=15&art=2&section=24A

Principles:

Minimum Necessary and Limited Use

1.21. Genetic Information Nondiscrimination Act of 2008 (GINA)

Internal Revenue Service, Department of Labor and Department of Health and Human Services joint regulations under Title I of GINA – 26 C.F.R. Part 54, 29 C.F.R. Part 2590 and 45 C.F.R. Parts 144, 146, and 148; and Equal Employment Opportunity Commission regulations under Title II of GINA – 29 C.F.R. Part 1635

Description:

The Genetic Information Nondiscrimination Act of 2008 (GINA), Public Law 110-233 (May 21, 2008), is designed to prohibit the improper use of genetic information in health insurance and employment. It prohibits group health plans and health insurers from denying coverage to a healthy individual or charging that person higher premiums based solely on a genetic predisposition to developing a disease in the future. The legislation also bars employers from using individuals' genetic information when making hiring, firing, job placement, or promotion decisions. Employers with fifteen (15) or more employees and entities affecting commerce must display a GINA informational poster on their premises, describing that employment discrimination based on genetic information is against the law.

The Internal Revenue Service, the Department of Labor and the Department of Health and Human Services issued joint regulations under Title I of GINA – 26 C.F.R. Part 54, 29 C.F.R. Part 2590 and 45 C.F.R. Parts 144, 146 and 148.

Title II of GINA prohibits covered employers from discriminating against employees based on genetic information. The Equal Employment Opportunity Commission (EEOC) issued regulations implementing Title II of the Act on November 9, 2010. These regulations are comprehensive. They describe or clarify:

1. Practices prohibited by GINA;
2. What constitutes "genetic information";
3. Examples of tests that would not be considered genetic tests;
4. Six narrowly-defined situations in which an employer may acquire genetic information;
5. Suggested warning language for employers to use when they request health-related information in the six narrowly-defined situations;
6. That there are no situations in which an employer may use genetic information to make employment decisions;
7. When acquisition of genetic information will be considered to be inadvertent;
8. What an employer must do to comply with GINA when lawfully requesting health-related information from an employee;
9. When an employer may ask for family medical history or other genetic information as part of a medical examination related to employment (*i.e.*, a post-offer or fitness-for-duty examination);

10. What an employer must do when it offers employees or his or her family members health or genetic services, including wellness programs, on a voluntary basis;
11. Why GINA includes an exception that allows an employer to acquire family medical history as part of the Family Medical Leave Act certification;
12. Types of situations when an employer may lawfully acquire genetic information from sources that are commercially and publicly available;
13. Circumstances in which an employer may acquire genetic information through genetic monitoring of its workforce;
14. Employer acquisition of genetic information for law enforcement purposes or for human remains identification;
15. GINA's rules on confidentiality;
16. The prohibition of disparate impact claims under Title II of GINA;
17. The prohibition on harassment based on genetic information;
18. Application of Title II of GINA to employment decisions concerning health care benefits, including a "firewall" provision intended to eliminate "double liability" by preventing claims asserted under Title II from also being asserted under Title I of GINA;
19. That GINA does not preempt any state or local law that provides equal or greater protections from employment discrimination on the basis of genetic information or that provide greater privacy protections;
20. Remedies available against an employer for violation of GINA Title II; and
21. What happens when an employee files a charge under GINA with the EEOC against a private sector employer or a state or local government employer.

On May 17, 2016, the EEOC published a final rule, effective January 1, 2017, relating to employer-sponsored wellness programs. The rule clarifies that an employer may offer a limited incentive (in the form of a reward or penalty) for an employee's spouse to provide information about the spouse's current or past health status as part of a voluntary wellness program.

GINA expands Title VII of the Civil Rights Act of 1964, which already bans discrimination by race and gender to prohibit employers from discriminating against employees on the basis of "genetic information" in hiring, firing, and other activities. "Genetic information" not only includes tests that determine variations in a person's DNA, but also information regarding family history of a particular disease. GINA also prohibits employers from collecting genetic information from their employees, except for rare circumstances such as testing for adverse effects to hazardous workplace exposures, and requires strict confidentiality of genetic information obtained by employers. GINA grants employees and individuals remedies similar to those provided under Title VII and other nondiscrimination

laws, i.e., compensatory and punitive damages. It also provides that no person shall retaliate against an individual for opposing an act or practice made unlawful by GINA. Currently, GINA does not prohibit discrimination once someone already has a disease.

GINA is far-reaching in that it amends or touches upon many laws including the Employee Retirement Income Security Act of 1974 (ERISA), the Public Health Service Act, the Internal Revenue Code of 1986, Title XVIII (Medicare) of the Social Security Act, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). For example, it amends ERISA and the Public Health Service Act to prohibit health insurers from discriminating against individuals on the basis of genetic information. It also prohibits insurers from requiring genetic testing, tying premiums to genetic information, or considering family history of genetic disorders in making underwriting and premium determinations.

GINA also required that the HIPAA Privacy Rule be amended to ensure that genetic information would be treated as health information and that Covered Entities would not use or disclose genetic information for underwriting purposes in certain health plans. In order to strengthen the privacy protections for genetic information, OCR incorporated these changes into its January 25, 2013, Omnibus Final Rule modifying HIPAA pursuant to the HITECH Act and GINA (*See* Section 1.4). Despite protest during the comment period, OCR also extended the prohibition on use of genetic information for underwriting purposes to all health plans that are Covered Entities, with the exception of long term care plans.

Implications:

- Departments shall develop procedures in compliance with GINA.
- Departments possessing genetic information about its employees must keep the information confidential and stored in separate files.
- Departments must develop protocols to maintain the confidentiality of genetic information unless the disclosure is to one of the following: (1) to the employee upon request; (2) to a health researcher; (3) as directed by a court order; (4) to a government official investigating compliance with GINA; or (5) in connection with federal and state family and medical leave act provisions.

Source:

Pub/ L. No. 110-233 – Genetic Information Nondiscrimination Act of 2008 (GINA) (May 21, 2008)
http://www.gpo.gov/fdsys/pkg/PLAW-110publ233/pdf/PLAW-110publ233.pdf

42 U.S.C. Chapter 140, Subchapter II – Exchange of Criminal History Records for Noncriminal Justice Purposes
http://www.law.cornell.edu/uscode/text/42/chapter-140/subchapter-II

29 C.F.R. Part 1635 – Genetic Information Nondiscrimination Act of 2008

http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=22ba5ac59948ddf4d5875ed1e8c0da2b&rgn=div5&view=text&node=29:4.1.4.1.21&idno=29

81 Fed. Reg. 31143 – Final Rule Amending Title II GINA regulations (May 17, 2016)
https://www.federalregister.gov/articles/2016/05/17/2016-11557/genetic-information-nondiscrimination-act

Questions and Answers Concerning Amendments to GINA Regulations
https://www.eeoc.gov/laws/regulations/qanda-gina-wellness-final-rule.cfm

29 C.F.R. Part 2590 – Rules and Regulations for Group Health Plans
http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title29/29cfr2590_main_02.tpl

Interim Final Rules Prohibiting Discrimination Based on Genetic Information in Health Insurance Coverage and Group Health Plans
Department of the Treasury, Internal Revenue Service,
26 C.F.R. Part 54, TD 9464, RIN 1545-BI03
Department of Labor, Employee Benefits Security Administration,
29 C.F.R. Part 2590, RIN 1210-AB27
Department of Health and Human Services, Centers for Medicare & Medicaid Services,
45 C.F.R. Parts 144, 146, and 148, RIN 0938-AP37
http://www.genome.gov/Pages/PolicyEthics/GeneticDiscrimination/GINA-HHSRegs-100209.pdf

Principles:
Accountability, Minimum Necessary and Limited Use, Consent, Individual Rights, Security Safeguards

1.22. Real ID Act of 2005

49 U.S.C. § 30301; 6 C.F.R. Part 37

Description:

The REAL ID Act of 2005, Public Law 109-13 (May 11, 2005), 49 U.S.C. § 30301, is a nationwide effort intended to prevent terrorism, reduce fraud, and improve the reliability and accuracy of identification documents that state governments issue. This law imposes certain security, authentication, and issuance procedure standards for states' driver's licenses and state ID cards in order for them to be accepted by the federal government for "official purposes," as defined by the Secretary of Homeland Security. Currently, the Secretary of Homeland Security has defined "official purposes" as presenting state driver's licenses and identification cards for boarding commercially operated airline flights, entering federal buildings, and entering nuclear power plants. The Act is a rider to an act titled Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005.

The final rule requires the states to have a comprehensive security plan for offices that have DMV records and information systems. The plan must safeguard personally identifiable information collected, stored, or disseminated for purposes of complying with the REAL ID Act, including procedures to prevent unauthorized access, use, or dissemination of applicant information and images of source documents. The regulations include standards and procedures for document retention and destruction. Also, the regulations include standards for the information and security features that must be incorporated into the ID card.

At present, all state issued licenses and identification cards have phased implementation dates commencing December 1, 2014, and the requirement for compliance with the REAL ID Act to board commercially operated airline flights will begin January 22, 2018, with full compliance required beginning October 1, 2020.

Note:

See also, Section 1.11 Driver's Privacy Protection Act

Implications:

- The Departments shall work with leadership to develop a driver's license and identification card in compliance with the Real ID Act's requirements.
- The Real ID Act anticipates the exchange of driver identity data, document imaging, digital photographs, and driver record information among all states accompanied by proper restrictions on any outside access or improper usage.

Source:

Pub. L. No. 109-13, REAL ID Act of 2005 (May 11, 2005)
https://www.gpo.gov/fdsys/pkg/STATUTE-119/pdf/STATUTE-119-Pg231.pdf

Department of Homeland Security – Privacy Impact Assessment for the REAL ID Act
https://www.dhs.gov/publication/real-id-privacy-impact-assessment

Department of Homeland Security – REAL ID Enforcement in Brief
https://www.dhs.gov/real-id-enforcement-brief

6 C.F.R. Part 37 – Real ID Driver's Licenses and Identification Cards
http://www.law.cornell.edu/cfr/text/6/37

Department of Homeland Security – REAL ID Frequently Asked Questions
http://www.dhs.gov/real-id-public-faqs

Principles:
Accountability, Notice, Minimum Necessary and Limited Use, Security Safeguards

1.23. Electronic Communications Privacy Act of 1986

18 U.S.C. § 2701, et seq.; 47 U.S.C. § 605

Description:

The Electronic Communications Privacy Act of 1986, and the Stored Wire Electronic Communications Act are commonly referred to together as the Electronic Communications Privacy Act of 1986 (ECPA). The ECPA updated the Federal Wiretap Act of 1968. The older Wiretap Act had been written to address interception of conversations using "hard" telephone lines. The onset of computer and other digital and electronic communications prompted the need to make the update. The USA PATRIOT Act and subsequent federal enactments have clarified and updated the ECPA in light of the ongoing development of modern communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically. ECPA has three titles:

- Title I of the ECPA is often referred to as the Wiretap Act, 18 U.S.C. §§ 2510 - 22
- Title II of the ECPA is called the Stored Communications Act (SCA), 18 U.S.C. §§ 2701- 12
- Titles III of the ECPA addresses pen register and trap and trace devices. 18 U.S.C. §§ 3121 - 27

This law was enacted to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. The Act prohibits persons from tampering with computers or accessing certain computerized records without authorization. The Act also prohibits providers of electronic communications services from obtaining, altering or preventing authorized access to stored electronic communications. The Stored Communications Act usually requires that the customer be notified and give an opportunity to contest in court a government entity's request for access to electronic mail or other stored communications in control of a provider of electronic communications services or remote computing services.

While the Act is, in part, a criminal anti-hacking statute, it also provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." The Act directly prohibits the interception of e-mail transmissions. Interception is prohibited by (1) unauthorized individuals or (2) individuals working for a government entity and acting without a

proper warrant. While there is no specific prohibition in the Act for an employer to monitor the e-mail of employees, it does not specifically exempt employers.
The Act has several exceptions to the application of the prohibition of interception of electronic communications. The three most relevant to the workplace are (1) where one party consents, (2) where the provider of the communication service can monitor communications, and (3) where the monitoring is done in the ordinary course of business.

Violators of the Act are subject to criminal penalties, including both fines and imprisonment. It also creates a civil cause of action for any "person aggrieved by any violation of this chapter" where the conduct constituting the violation "is engaged in with a knowing or intentional state of mind."

Implications:

- Departments will establish clear, concise policies limiting employees' privacy in their electronic communications while using workplace computer systems.
- Departments will notify employees of their limited expectation of privacy in their personal communications on the workplace service provider and that the Department as the provider of the equipment and services, retains the right to monitor the equipment's usage.
- Departments should notify employees that anyone in violation of the Computer and Internet Use policies will be disciplined.
- Departments should have employees sign a written acknowledgement that they have received, read and accepted the computer usage policies.
- *See* Federal Case Law Section 2.0(B) *City of Ontario v. Quon*

Source:

18 U.S.C. §§ 2510-22 – Wire and Electronic Communications Interception and Interception of Oral Communications
http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119

18 U.S.C. §§ 2701-12 – Stored Wire and Electronic Communications and Transactional Records Access
http://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

18 U.S.C. §§ 3121-27 – Pen Registers and Trap and Trace Devices
https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206

47 U.S.C. § 605 – Unauthorized publication or Use of Communications
http://www.law.cornell.edu/uscode/text/47/605

Congressional Research Service Report R41733 – Privacy: An Overview of the Electronic Communications Privacy Act (October 9, 2012)
http://www.fas.org/sgp/crs/misc/R41733.pdf

The Act was amended by 47 U.S.C. §§ 1001-10
http://www.law.cornell.edu/uscode/text/47/chapter-9/subchapter-I

Principles:
Notice, Consent

1.24. Federal Aviation Administration

14 C.F.R. Part 107

Description:

In 2016, the Department of Transportation's Federal Aviation Administration (FAA) finalized rules for routine commercial use of small unmanned aircraft systems (UAS), commonly known as "drones." UAS technology has rapidly brought efficiency and productivity to the daily lives of individuals and businesses. The substantial benefits of commercial and private operations of UAS encouraged the FAA to implement new safety regulations for unmanned aircraft systems weighing less than 55 pounds.

Aside from bringing substantial benefits to both the commercial and private industries, UAS technology integration has raised privacy issues, and FAA recognizes the importance of addressing these concerns. However, FAA's rulemaking authority is limited to the critical aviation safety concerns. FAA's rulemaking authority does not permit FAA to issue or enforce regulations aimed at protecting privacy interests.

Although FAA's new regulations do not address the privacy issues related to the use of UAS, the FAA has taken part in a privacy education program, in which the agency provides recommended privacy guidelines. The FAA participated in and relied on the National Telecommunication and Information Administration's published efforts, commonly referred to as "voluntary Best Practices," as a way to advance the best practices for privacy, transparency, and accountability issues regarding commercial and private UAS use.

The voluntary Best Practices are not meant to create a legal standard, but instead, provide a guideline to encourage all UAS operators to comply with all applicable laws and regulations and protect evolving privacy expectations. More specifically, the voluntary Best Practices aims to protect covered data, which is information collected by a UAS that identifies a particular person by their name or other personally identifiable information. The voluntary Best Practices encourage both commercial and private UAS operators to make five practical and reasonable efforts while operating UAS. UAS operators should:

- Make reasonable efforts to provide notice to others of their use of UAS.
- Show care when operating UAS or collecting and storing covered data from UAS by: (1) avoiding the use of UAS for the specific purpose where the operator knows the data subject has reasonable expectation of privacy; (2) avoiding the use of UAS for specific purpose of persistent and continuous collection about individuals; (3) making reasonable efforts to minimize UAS operations over and within private property without owner's consent; (4) making reasonable effort not to retain covered data longer than reasonably

necessary; and (5) establishing a process for receiving privacy and security concerns.

- Limit the use and sharing of covered data unless the data subject provides consent to the use or disclosure.
- Secure the covered data by implementing a program that contains reasonable and appropriate administrative, technical, and physical safeguards. The safeguards should include: (1) written security policies with respect to the collection, use, storage, and dissemination of covered data; (2) efforts to monitor those systems, and (3) authorized access.
- Monitor and comply with evolving federal, state, and local UAS laws.

Implications:

- Departments should protect evolving privacy expectations while operating UAS by providing notice, respecting other people's rights to privacy, and establishing reasonable policies and safeguards.
- Departments should provide security training to employees that have authorized access to covered data, which is information collected by a UAS that identifies a particular person.
- Departments should comply with all applicable laws and regulations in operating UAS.

Source:

Voluntary Best Practices for UAS Privacy, Transparency, and Accountability – http://www.ntia.doc.gov/files/ntia/publications/voluntary_best_practices_for_uas_privacy_transparency_and_accountability_0.pdf

Press Release – DOT and FAA Finalize Rules for Small Unmanned Aircraft Systems – https://www.faa.gov/news/press_releases/news_story.cfm?newsId=20515

Part 107 Rule updated – www.faa.gov/uas/media/RIN_2120-AJ60_Clean_Signed.pdf

Principles:

Consent, Privacy Safeguards, Transparency, Accountability, Minimum Necessary and Limited Use

2.0. Federal Case Law

A. Freedom of Information Act (FOIA)

1. *FCCl v. AT&T Inc*., 562 U.S. 397, 131 S. Ct. 1177, 179 L. Ed. 2d 132 (2011).

In 2004, AT&T and FCC agreed to produce an “E-Rate” program that assists schools and libraries across the US to obtain affordable telecommunications and Internet access. Subsequently, AT&T disclosed to FCC that it might have overcharged for its services under this program. The FCC conducted an investigation that led to a $500,000 settlement being paid by AT&T. A number of AT&T customers, represented by CompTel Company, then requested the FCC to make public all the pleadings and correspondences between FCC and AT&T from the investigation. AT&T challenged the request relying on two exemptions in the Freedom of Information Act, § 552(b)(4), which excuses disclosure of trade secrets and commercial or financial information, and § 552(b)(7)(C), which exempts law enforcement records the disclosure of which would constitute an unwarranted invasion of personal privacy. The FCC concluded that "Exemption 7(C) has no applicability to corporations such as AT&T.” AT&T appealed the FCC’s decision to the Third Circuit Court of Appeals. There, the FCC argued that while AT&T should be afforded some protection under §522(b)(4), AT&T should not be allowed the exemption afforded under § 522(b)(7)(C) because a corporation is not considered a person and therefore the exemption does not apply. Conversely, AT&T argued that Congress had previously defined the word "person" to include corporations, and therefore, corporations are entitled to the exemption. The Third Circuit agreed with AT&T, and the FCC appealed to the United States Supreme Court.

The Supreme Court, in a unanimous decision, reversed the decision of the Circuit Court finding that while corporations may be entitled to personal rights against unreasonable search and seizure under the Fourth Amendment and freedom from double jeopardy, these rights are not extended to FOIA's personal privacy exemption. Additionally, the Court explained that while Congress intended for § 522(b)(4) to apply to corporations, § 522(b)(7)(C) was intended only to apply to the privacy rights of individuals. Accordingly, the exemption afforded under § 522(b)(7)(C) for personal privacy is not extended to corporations and the FOIA disclosure was authorized.

2. *Milner v. Dep’t. of the Navy*, 562 U. S. 562, 131 S. Ct. 1259, 179 L. Ed. 2d 268 (2011).

Glen Milner, a member of an organization dedicated to raising community awareness about the dangers of Navy training exercises near Puget Sound, sued the Department of the Navy in a Washington federal district court under the Freedom of Information Act ("FOIA") to obtain the release of Navy documents relating to the effects of explosions at several locations. The district court granted

summary judgment in favor of the Navy. On appeal, the U.S. Court of Appeals for the Ninth Circuit affirmed, holding that documents relating to the effects of explosions constituted “internal personnel rules and regulations of an agency” which are subject to exemption from disclosure under the FOIA. The court reasoned that such documents are "predominantly" for internal agency use and present a risk that, if disclosed, they would circumvent agency regulation.

Before the United States Supreme Court, the issue was whether the Ninth Circuit Court of Appeals erred by exempting documents relating to the effects of explosions from disclosure under the FOIA because they are "predominantly" for internal use and present a risk of circumventing agency regulation.

The Supreme Court answered this question in the affirmative, reversing the lower court decision, in an 8-1 opinion written by Justice Kagan. The majority opinion held that "because Exemption 2 encompasses only records relating to employee relations and human resources issues, the explosives maps and data requested here do not qualify for withholding under that exemption."

Justice Alito filed a concurring opinion, in which he agreed with the judgment but noted: "I write separately to underscore the alternative argument that the Navy raised below, which rested on Exemption 7(F) and which will remain open on remand." Justice Breyer dissented, backing the decision of the appeals court.

Note: In *Pub. Emps. for Envtl. Responsibility v. Int’l Boundary & Water Comm’n*, 740 F.3d 195 (D.C. Cir. 2014), the D.C. Circuit examined similar issues presented in Milner under alternative exemptions to the “internal personnel rules and regulations of an agency.” Instead, the Circuit Court held that records and documents related to two dams on the border of the United States and Mexico were exempt from disclosure under Exemption 7, “records or documents compiled for law enforcement purposes.” The Court’s analysis on the application of 7(E) and 7(F) is in line with Justice Alito’s concurring opinion in Milner.

Implications:
These decisions should be considered when interpreting any similar provisions within West Virginia’s Freedom of Information Act.

B. Privacy

1. *City of Ontario v. Quon*, 560 U.S. 746, 130 S. Ct. 2619, , 177 L. Ed. 2d 216 (2010).

Employees of the City of Ontario, California police department filed a 42 U.S.C. § 1983 claim in a California federal district court against the police department, city, chief of police, and an internal affairs officer. They alleged Fourth Amendment violations in relation to the police department's review of text messages made by an employee on a city issued text-message pager. While the city did not have an official text-messaging privacy policy, it did have a general "Computer Usage,

Internet, and E-mail Policy." The policy in part stated that "[t]he City of Ontario reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice," and that "[u]sers should have no expectation of privacy or confidentiality when using these resources." Employees were told verbally that the text-messaging pagers were considered e-mail and subject to the general policy. The district court entered judgment in favor of the defendants.

On appeal, the U.S. Court of Appeals for the Ninth Circuit reversed in part. The court held that city employees had a reasonable expectation of privacy for the text messages they sent on their city-issued pagers because there was no text message privacy policy in place. Additionally, the court noted that the police department's review of the text messages was unreasonable because it could have used "less intrusive methods" to determine whether employees had properly used the text messaging service.

On appeal, the United States Supreme Court was asked to address two questions:

(1) Does a city employee have a reasonable expectation of privacy in text messages transmitted on his city-issued pager when the police department has no official privacy policy for the pagers?

(2) Did the Ninth Circuit contravene Supreme Court precedent by analyzing whether the police department could have used "less intrusive methods" of reviewing text messages?

The Supreme Court did not answer the first question because it unanimously upheld the legality of the Ontario, California Police Department's audit of a police sergeant's text messages in his department-issued pager. Declining to issue a broad holding on employee privacy rights in electronic communications, the Court decided the case on the narrow point that, even assuming that the employee had a reasonable expectation of privacy in his text messages, the search was reasonable because it was motivated by a legitimate, work-related purpose and was not excessive in scope. The opinion emphasized, however, the importance of well-crafted employer privacy policies, noting that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."

The *Quon* decision contained the following additional comments:

The Court, in light of the department's policy in this case, highlighted the distinction between e-mails that are transmitted through a company's own server and text messages that are transmitted through a wireless provider's network but ultimately concluded that the policy covered both;

The Court noted that the department's audit of Quon's text messages on his employer-provided pager was "not nearly as intrusive as a search of his personal e-mail account or page or a wiretap on his home phone line";

The Court noted with approval the City's removal of the employee's off-duty messages from the audit and confinement of the audit to two months; and

The Court made clear that it has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."

Note: A Texas court recently declined to extend the holding in *Quon* to a newspaper's request for email correspondence related to the "Commissioner's official capacity as a county commissioner." *See Adkisson v. Paxton*, 2015 WL 1030295 (Tex. Ct. App. 2015). The court held that emails from personal accounts, if related to official business, are subject to the state's Public Information Act (PIA).

A Wisconsin court recently distinguished *Quon* and other cases where a reasonable expectation of privacy in text messages on a cell phone exists. *See State v. Tentoni*, 871 N.W.2d, 285 (Wis. Ct. App. 2015). The court held that an individual had no privacy right to text messages found on another person's phone.

Implications:

Departments should either clarify and update or implement written policies covering all forms of electronic communications and require written acknowledgements of receipt by employees.

Department privacy policies should state that employees do not have an expectation of privacy in electronic communications sent or received on Department-provided devices and that the Department may monitor and review electronic communications sent on such devices, not just those sent through the Department's server.

Privacy policies should state that they can only be amended in writing by certain specified individuals with designated authority and should provide that violations of the privacy policies may lead to discipline up to and including termination.

Departments should consider whether their privacy policies pertaining to workplace monitoring and surveillance clearly state when (defining purpose and scope) Departments may conduct legitimate and reasonable searches of Department-provided service and equipment.

Departments should provide training regarding the electronic communications policy to all employees.

Departments should consider developing investigative protocols for vetting, conducting and limiting searches, documenting the purpose for such searches, and establishing minimization procedures in order to enhance the likelihood that

such searches will be deemed compliant in light of *Quon* and general privacy notions.

Departments should be aware that even if a document is sent from a personal device outside of working hours, it may be subject to discovery under a state act like PIA or FOIA.

2. *National Aeronautics and Space Administration v. Nelson*, 562 U.S. 134, 131 S. Ct. 746, 178 L. Ed. 2d 667 (2011).

A 2004 Bush administration antiterrorism initiative extended background checks required for many government jobs to contract employees, including scientists and engineers at the Jet Propulsion Laboratory, a research facility operated by the California Institute of Technology under a contract with NASA. Twenty-eight lab employees, who did not have security clearances and were not involved in classified or military activities, filed suit over what they considered to be overly intrusive background checks contending that the background check process violated a constitutional right to informational privacy for contract employees. The forms at issue asked whether an employee had "used, possessed, supplied, or manufactured illegal drugs" in the last year. If so, the employee was required to provide details, including information about "treatment or counseling received." An employee was also required to sign a release authorizing the Government to obtain personal information from schools, employers, and others during its investigation. The Government sent the references provided by the employee a questionnaire asking open-ended questions about whether the references had "any reason to question" the employee's "honesty or trustworthiness" or had "adverse information" concerning a variety of other matters. All responses on the forms were subject to the protections of the federal Privacy Act.

A three-judge panel of the U.S. Court of Appeals for the Ninth Circuit ordered the background checks halted while the case continued. The divided court later declined an *en banc* review.

The Supreme Court reversed the Ninth Circuit's reversal of the district court's denial of a preliminary injunction. The Court determined that while the government's challenged inquiries implicated a privacy interest of constitutional significance, that interest did not prevent the government from asking reasonable questions of the sort included on the forms at issue in an employment background investigation that was subject to the Privacy Act's safeguards against public disclosure.

Specifically, the Court noted that the challenged questions were reasonable, employment-related inquiries that further the Government's interests in managing its internal operations. The "treatment or counseling" question was a follow-up question to a reasonable inquiry about illegal-drug use. The drug-treatment inquiry was also a reasonable, employment-related inquiry. Additionally, the form's open-ended questions were reasonably aimed at identifying capable and reliable

employees. The Court concluded: "the Government has an interest in conducting basic employment background checks. Reasonable investigations of applicants and employees aid the Government in ensuring the security of its facilities and in employing a competent, reliable workforce."

The Court found significant that the answers to the Government's background check forms were subject to substantial protections against disclosure to the public. The Court noted that the Privacy Act allows the Government to maintain only those records "relevant and necessary to accomplish" a purpose authorized by law and requires written consent before the Government may disclose an individual's records.

Implications:

The Supreme Court's decision confirms that Departments may request a broad range of background information from employees or applicants, as long as the inquiry is related to the Department's interest in employing a competent workforce. However, Departments must take meaningful steps to comply with state and federal privacy laws and protect collected confidential information from disclosure.

3. *United States v. Jones*, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012).

In *Jones*, the United States Supreme Court revived the doctrine that a physical intrusion by the government into a constitutionally protected area for the purpose of gathering information is a Fourth Amendment search, a principle most courts had considered subsumed by the reasonable expectation of privacy standard. As part of a drug conspiracy investigation, officers obtained a warrant from the U.S. District Court for the District of Columbia to install a tracking device on a vehicle used by Jones but registered to his wife. The tracking device was to be placed on the vehicle within 10 days. Eleven days after the court order was issued, officers placed the GPS device on the vehicle while it was in Maryland. The device provided officers with 2,000 pages of location data over the next four weeks. Jones' motion to suppress the GPS information was denied; he was convicted and then appealed. The court of appeals reversed the conviction, finding the warrantless use of the GPS device in violation of the Fourth Amendment. The appellate court held that the use of the GPS device was a search where Jones had a reasonable expectation of privacy in his movements over an extended period of time.

The Supreme Court unanimously agreed that the use of the GPS was a search under the Fourth Amendment, but filed separate opinions with divergent reasoning in support of that conclusion. The majority opinion written by Justice Scalia relied on an originalist interpretation finding the vehicle to be an "effect" within the meaning of the Fourth Amendment and the attachment of the GPS device to a vehicle by government agents to gather information to be a trespass and, therefore, a search within the meaning of the Fourth Amendment. "The government physically occupied private property for the purpose of obtaining information. [The Court had] no doubt that such a physical intrusion would have

been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." The opinion expresses that the original theory of governmental trespass as a basis for a Fourth Amendment violation had not been replaced by the theory of "reasonable expectation of privacy" developed in *United States v. Katz*, 389 U.S. 347, 88 S. Ct. 507, 19 L.. Ed. 2d 576 (1967). In *Katz* the court found that the government had violated the Fourth Amendment by placing a covert microphone on a public phone booth, without a warrant, to overhear a suspect's telephone conversation. *Katz* and cases following it expanded the protection of the Fourth Amendment beyond "persons, houses, papers, and effects" (as expressly listed in the Fourth Amendment) and held that the amendment protected people and their reasonable expectation of privacy in less concrete matters, like conversations, telephone calls, and e-mails.

Prior to the Supreme Court's decision in *Jones*, several federal circuit court decisions held that people had no reasonable expectation of privacy in the movement of their vehicles on public streets because those actions are readily observable by anyone—including the government—and, therefore, use of a GPS device to monitor a vehicle's movement on public streets did not violate any reasonable expectation of privacy. In each of those cases, the courts had held that the act of the physical installation itself of a slap-on or magnetic GPS device on the vehicle did not independently constitute a search under the Fourth Amendment. *Jones* overruled these decisions when placing a tracking device on the vehicle required a physical touching of the vehicle with the intention of gathering information. The Court did not overrule prior decisions where the tracking device was already in place before the subject took possession of the object to be tracked because there was no trespass. The *Jones* decision leaves open the question of the constitutionality of electronic tracking, which is feasible by nonphysical means, such as monitoring a subject's movements through GPS signals emitted by a cellular telephone.

Justice Sotomayor joined with the majority opinion in holding that here the physical trespass on a constitutionally protected "effect" (the vehicle) constituted a Fourth Amendment search but filed a concurring opinion agreeing with Justice Alito's concurrence that long-term GPS monitoring would infringe on an individual's reasonable expectation of privacy. Justice Sotomayor also expressed that in other cases not involving physical intrusion, the *Katz* approach should be applied given concern regarding data aggregation and government accumulation of information.

Justice Alito filed an opinion concurring in the result, which was joined by three other justices, but believed the case should be decided by applying the *Katz* reasonable expectation of privacy analysis. He also reasoned that the long-term monitoring of the movement of Jones' vehicle violated his reasonable expectation of privacy. Justice Alito's opinion suggests that the reasonable expectation of privacy analysis would encompass all types of surveillance, including old fashioned physical surveillance with cars and aircraft, as well as tracking, which could be achieved remotely as opposed to the need to physically intrude into a protected

area. It also indicates that how long citizens can be followed may differ based on the offense being investigated. While not delineating a matrix of time limits that would be allowable for different offenses, Justice Alito indicated that 28 days was too long in this case, involving a drug investigation.

Jones was decided by applying a simple trespass analysis. However, five justices signaled readiness to expand the protections of the Fourth Amendment in future cases to limit government collection and aggregation of publicly available information where such efforts may violate the public's reasonable expectation of privacy.

Note: In *Grady v. North Carolina*, the Supreme Court examined whether attaching a device to a recidivist sex offender that would monitor his movements by satellite for the remainder of his life violated due process. 135 S. Ct. 1368 (2015). Grady was a sex offender, who upon release from prison was ordered to wear a satellite-based monitoring device. He sued claiming his due process rights were violated and that it violated his privacy rights. The Supreme Court stated that because the purpose of the program was to collect information about Grady it was undoubtedly a search, and required due process protection. Additionally, the Supreme Court focused on the fact that if attaching a device to a car was a trespass, attaching one to one's person would also be. However, the Supreme Court left unanswered the question of whether it was reasonable to attach such a device for remand. *See also* United States v. Graham, No. 12-4659, 2016 WL 3068018 (4th Cir. May 31, 2016) (en banc) (holding that, under the third-party doctrine applicable to Fourth Amendment searches, an individual lacks a reasonable expectation of privacy in historical cell phone site location information because the information was voluntarily conveyed to a third party (the defendants' cell phone provider) by making and receiving calls and texts on their phones), and therefore, does not require a warrant); *United States v. Weast*, 811 F.3d 743 (5th Cir. 2016) (holding that child pornographer had no reasonable expectation of privacy in IP address or files shared on peer-to-peer network).

4. *Florida v. Harris*, 133 S. Ct. 1050, 185 L. Ed. 2d 61 (2013).

In *Harris*, the United States Supreme Court considered whether the "alert" of a drug-detection dog during a traffic stop provides probable cause to search a vehicle. The Florida Supreme Court held that the State must in every case present an exhaustive set of records, including a log of the dog's performance in the field, to establish the dog's reliability. *See* 71 So. 3d 756, 775 (2011). The United States Supreme Court reversed, finding the Florida Court's standard to be inconsistent with the "flexible, common-sense standard" of probable cause. *Illinois v. Gates*, 462 U. S. 213, 239 (1983).

The material facts were that William Wheetley, a K–9 Officer in the Liberty County, Florida Sheriff's Office, was on a routine patrol with Aldo, a German shepherd trained to detect certain narcotics (methamphetamine, marijuana, cocaine, heroin,

and ecstasy). Wheetley pulled over respondent Clayton Harris's truck because it had an expired license plate. On approaching the driver's-side door, Wheetley saw that Harris was "visibly nervous," unable to sit still, shaking, and breathing rapidly. Wheetley also noticed an open can of beer in the truck's cup holder. Wheetley asked Harris for consent to search the truck, but Harris refused. At that point, Wheetley retrieved Aldo from the patrol car and walked him around Harris's truck for a "free air sniff." Aldo alerted at the driver's-side door handle signaling, through a distinctive set of behaviors, that he smelled drugs there. Wheetley concluded, based principally on Aldo's alert, that he had probable cause to search the truck. His search did not turn up any of the drugs Aldo was trained to detect. But it did reveal 200 loose pseudoephedrine pills, 8,000 matches, a bottle of hydrochloric acid, two containers of antifreeze, and a coffee filter full of iodine crystals -- all ingredients for making methamphetamine. Wheetley then arrested Harris, who admitted after proper Miranda warnings that he routinely "cooked" methamphetamine at his house and could not go more than a few days without using it. The State charged Harris with possessing pseudoephedrine for use in manufacturing methamphetamine. While out on bail, Harris had another run-in with Wheetley and Aldo. This time, Wheetley pulled Harris over for a broken brake light. Aldo again sniffed the truck's exterior, and again alerted at the driver's-side door handle. Wheetley once more searched the truck, but on this occasion discovered nothing of interest. At trial, Harris moved to suppress the evidence found in his truck on the ground that Aldo's alert had not given Wheetley probable cause for a search. At the hearing on that motion, Wheetley testified about both his and Aldo's training in drug detection. In 2004, Wheetley (and a different dog) completed a 160-hour course in narcotics detection offered by the Dothan, Alabama Police Department, while Aldo (and a different handler) completed a similar, 120-hour course given by the Apopka, Florida Police Department. That same year, Aldo received a one-year certification from Drug Beat, a private company that specializes in testing and certifying K–9 dogs. Wheetley and Aldo teamed up in 2005 and went through another 40-hour refresher course in Dothan together. They also did four hours of training exercises each week to maintain their skills. Wheetley would hide drugs in certain vehicles or buildings while leaving others "blank" to determine whether Aldo alerted at the right places. According to Wheetley, Aldo's performance in those exercises was very good. The State introduced "Monthly Canine Detection Training Logs" consistent with that testimony. The logs showed that Aldo always found hidden drugs and that he performed "satisfactorily" (the higher of two possible assessments) on each day of training. On cross-examination, Harris's attorney chose not to contest the quality of Aldo's or Wheetley's training. Instead, she focused on Aldo's certification and his performance in the field, particularly the two stops of Harris's truck. Wheetley conceded that the certification (which, he noted, Florida law did not require) had expired the year before he pulled Harris over. Wheetley also acknowledged that he did not keep complete records of Aldo's performance in traffic stops or other field work. Instead, he maintained records only of alerts resulting in arrests. Wheetley defended Aldo's two alerts to Harris's seemingly narcotics-free truck:

According to Wheetley, Harris probably transferred the odor of methamphetamine to the door handle, and Aldo responded to that residual odor.

The trial court concluded that Wheetley had probable cause to search Harris's truck and denied the motion to suppress. Harris then entered a no-contest plea while reserving the right to appeal the trial court's ruling. An intermediate state court summarily affirmed. *See* 989 So. 2d 1214, 1215 (2008) (per curiam).

The Florida Supreme Court reversed, holding that Wheetley lacked probable cause to search Harris's vehicle under the Fourth Amendment. "[W]hen a dog alerts," the court wrote, "the fact that the dog has been trained and certified is simply not enough to establish probable cause." 71 So. 3d at 767. To demonstrate a dog's reliability, the State needed to produce a wider array of evidence:

"[T]he State must present . . . the dog's training and certification records, an explanation of the meaning of the particular training and certification, field performance records (including any unverified alerts), and evidence concerning the experience and training of the officer handling the dog, as well as any other objective evidence known to the officer about the dog's reliability." *Id*. at 775.

The court particularly stressed the need for "evidence of the dog's performance history," including records showing "how often the dog has alerted in the field without illegal contraband having been found." *Id.* at 769. That data, the court stated, could help to expose such problems as a handler's tendency (conscious or not) to "cue [a] dog to alert" and "a dog's inability to distinguish between residual odors and actual drugs." *Id*. at 769, 774. Accordingly, an officer like Wheetley who did not keep full records of his dog's field performance could never have the requisite cause to think "that the dog is a reliable indicator of drugs." *Id*. at 773.

The United State Supreme Court in a unanimous decision reversed finding that a police officer has probable cause to conduct a search when "the facts available to [him] would 'warrant a [person] of reasonable caution in the belief" that contraband or evidence of a crime is present. *Texas v. Brown*, 460 U. S. 730, 742 (1983) (plurality opinion) (quoting *Carroll v. United States*, 267 U. S. 132, 162 (1925)); *see Safford Unified School Dist. #1 v. Redding*, 557 U. S. 364, 370-371 (2009). The Court said that the test for probable cause is not reducible to "precise definition or quantification." *Maryland v. Pringle*, 540 U. S. 366, 371 (2003). "Finely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence . . . have no place in the [probable-cause] decision." *Gates*, 462 U. S., at 235. All we have required is the kind of "fair probability" on which "reasonable and prudent [people,] not legal technicians, act." *Id*. at 238, 231 (internal quotation marks omitted). The Court wrote that "in evaluating whether the State has met this practical and commonsensical standard, we have consistently looked to the totality of the circumstances." *See, e.g., Pringle*, 540 U. S., at 371; *Gates*, 462 U. S., at 232; *Brinegar v. United States*, 338 U. S. 160, 176 (1949). The Court has rejected rigid rules, bright-line tests, and mechanistic inquiries in favor of a more flexible,

all-things-considered approach. In *Gates*, for example, the Court abandoned its old test for assessing the reliability of informants' tips because it had devolved into a "complex superstructure of evidentiary and analytical rules," any one of which, if not complied with, would derail a finding of probable cause. 462 U. S. at 235. The Court lamented the development of a list of "inflexible, independent requirements applicable in every case." *Id*. at 230 n.6. The Court emphasized that probable cause is "a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Id*. at 232.

Note: In *United States v. Thomas*, the Second Circuit examined the issue of whether reliance on a computer program that monitored P2P networks to identify child pornography created sufficient probable cause. No. 14-1083-cr., 2015 WL 3619820 (2nd Cir. 2015). The defendant in that case attempted to rely on *Harris* by stating that the Supreme Court required certification for probable cause. However, the Second Circuit found that computer programs are different from dogs and do not need this kind of certification and performance training. According to the Second Circuit, because there was no evidence the computer program reports false or misleading information, there was sufficient 'indicia of reliability.'

5. *Florida v. Jardine*, 133 S. Ct. 1409, 185 L. Ed. 2d 495 (2013).

In *Jardine*, police took a drug-sniffing dog to Jardine's front porch, where the dog gave a positive alert for narcotics. Based on the alert, the officers obtained a warrant for a search, which revealed marijuana plants. Jardine was charged with trafficking in cannabis. The Supreme Court of Florida upheld the trial court's decision to suppress the evidence, holding that the officers had engaged in a Fourth Amendment search unsupported by probable cause.

The United States Supreme Court affirmed, writing that the investigation of Jardine's home was a "search" within the meaning of the Fourth Amendment. The decision makes the following points:

(1) When "the Government obtains information by physically intruding" on persons, houses, papers, or effects, "a 'search' within the original meaning of the Fourth Amendment" has "undoubtedly occurred." *United States v. Jones*, 565 U. S. 950-51 (2012).

(2) At the Fourth Amendment's "very core" stands "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." *Silverman v. United States*, 365 U. S. 505, 511. The area "immediately surrounding and associated with the home"—the curtilage—is "part of the home itself for Fourth Amendment purposes." *Oliver v. United States*, 466 U. S. 170, 180. The officers entered the curtilage here: The front porch is the classic exemplar of an area "to which the activity of home life extends." *Id*. at 182n.12.

(3) The officers' entry was not explicitly or implicitly invited. Officers need not "shield their eyes" when passing by a home "on public thoroughfares," *California v. Ciraolo*, 476 U. S. 207, 213, but "no man can set his foot upon his neighbor's close without his leave," *Entick v. Carrington*, 2 Wils. K. B. 275, 291, 95 Eng. Rep. 807, 817. A police officer not armed with a warrant may approach a home in hopes of speaking to its occupants, because that is "no more than any private citizen might do." *Kentucky v. King*, 131 S. Ct. 1849, 179 L. Ed. 2d 865 (2011). However, the scope of a license is limited not only to a particular area but also to a specific purpose, and there is no customary invitation to enter the curtilage simply to conduct a search.

(4) It is unnecessary to decide whether the officers violated Jardine's expectation of privacy under *Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).

6. *Maryland v. King*, 133 S. Ct. 1958, 186 L. Ed. 2d 1 (2013)

In *Maryland v. King*, the Supreme Court reached the question of "whether the Fourth Amendment prohibits the collection and analysis of a DNA sample from persons arrested, but not yet convicted, on felony charges." In 2009, the defendant was arrested and charged with first- and second-degree assault after he threatened a group of people with a shotgun. Pursuant to the Maryland DNA Collection Act (the Act), he was cheek swabbed for DNA during booking, and the DNA was later found to match the DNA sample from an unsolved rape in 2003. Based on that DNA evidence, the defendant was tried and convicted for the 2003 rape after the Circuit Court Judge denied his motion to suppress the DNA evidence because the Act violated the Fourth Amendment. The Maryland Court of Appeals reversed, deciding that the portions of the Act authorizing collection of DNA from felony arrestees were unconstitutional. It found the DNA collection unreasonable because the defendant's "expectation of privacy is greater than the State's purported interest in using [the defendant's] DNA to identify him."

In a 5-4 decision, the majority opinion by Justice Kennedy reversed the decision of the Maryland Court of Appeals. The Court began by detailing the effectiveness and precision of DNA testing as a means of identification. It also noted that the Combined DNA Index System (CODIS) was a growing means of maintaining reliable and standardized DNA identification information. The Court conceded that a cheek swab for DNA is definitely a search under the meaning of the Fourth Amendment and that the neutral nature of such a search meant that obtaining a warrant from an unbiased magistrate would be of little use. Because the cheek swab did not require a warrant, the Court concluded that the search should be analyzed under the traditional standards of reasonableness to determine whether the legitimate government interest outweighed the degree of intrusion on individual privacy.

The Court framed the legitimate government interest of the Act as "the need for law enforcement officers in a safe and accurate way to process and identify the persons and possessions they must take into custody." According to the court, the government interest in DNA identification was justified by the following: the need to know who has been arrested and who will be tried; the law enforcement responsibility to keep staff, existing detainees, and the new detainee safe; the concern that the accused will flee from custody; the need to use an arrestee's past conduct to determine if he poses a danger to the public; and the possibility that an innocent person will be vindicated by the identification of a guilty perpetrator. The Court noted the previous Constitutional methods of photography and measurements that police have used to identify criminals, and it also pointed out that fingerprinting had long been held as a Constitutional and effective means of identification. Accordingly, the Court concluded that it would be unreasonable to allow fingerprinting but disallow the much more effective means of DNA identification; therefore, it afforded great weight to the government interest at stake.

In regards to the degree of intrusion on individual privacy, the Court found that a cheek swab was a brief intrusion that did "not increase the indignity already attendant to normal incidents of arrest." Although such an intrusion is subject to the Fourth Amendment, it is reasonable in a custodial arrest where expectations of privacy are considerably lower. Therefore, the Court held that the state's interest in identification far outweighed the minor intrusion of a cheek swab, and DNA identification could be "considered part of a routine booking procedure" where an arrest is made upon probable cause for a serious offense.

Justice Scalia penned a vehement dissenting opinion, accusing the Court of allowing suspicionless searches with no "justifying motive apart from the investigation of crime." He argued that Maryland's DNA Act was never meant to identify arrestee's and was, in fact, never used for that purpose. Whereas fingerprinting is used to quickly disclose a person's identity, DNA testing is used to check against unsolved crimes; DNA testing takes too long and is not structured to facilitate the identification of arrestees. According to Scalia, "suspicionless searches are never allowed if their principal end is ordinary crime-solving." In his opinion, the Court's reasoning that DNA testing is justified by a state interest in identification was simply not supported by any actual use of the DNA for identifying purposes.

Note: In *Birchfield v. North Dakota*, the Supreme Court held that the Fourth Amendment permits warrantless breath tests incident to arrests for drunk driving but not warrantless blood tests. 136 S. Ct. 2160 (2016). The Court distinguished blood tests from breath tests as significantly more intrusive than the minimally inconvenient action of breathing into a mouthpiece. Among many factors leading to the decision, the Court noted that a breath test would not leave identifiable biological material behind.

Implications:
At the very least, states may implement legislation and regulations that require DNA samples to be taken as part of a routine booking procedure for those arrestees that are suspected of serious offenses. The Maryland Act upheld by the court authorized collection of DNA samples from those who are charged with a crime of violence or burglary; crimes of violence in Maryland include murder, rape, first-degree assault, kidnaping, arson, sexual assault, and a variety of other serious crimes. As Scalia mentions in his dissent, it is possible that the reasoning of "identification" presented in this case will be extended to other arrestees or individuals, but that is not yet the case.

7. *Fernandez v. California*, 134 S. Ct. 1126, 188 L.E.d.2d 25 (2014)

It is well settled that police may search jointly occupied premises if one of the occupants consent, but the Court has found an exception where one occupant consents and another present occupant objects. This case involved the question of whether police may search premises "if the objecting occupant is absent when another occupant consents." The material facts are that the defendant was arrested on suspicion of assault and in connection with the investigation of a robbery. Immediately prior to his arrest, the defendant objected to a search of his apartment, but police officers returned after the arrest and received consent from the defendant's cohabitant to search the apartment where they found a firearm and ammunition. The defendant's motion to suppress the evidence found in his apartment was denied, and he pled *non contendere* to possession of a firearm by a felon, possession of a short-barreled shotgun, and felony possession of ammunition. The California Court of Appeals affirmed, and the Supreme Court granted certiorari after the petition for review was denied by the California Supreme Court.

The Court, through Justice Alito, began by noting that consent searches are a well-established and constitutionally permissible warrantless search. Police officers may search jointly occupied premises if one of the occupants consents, and that search will be upheld even if the consenting "occupant" is later determined to not be a resident of the premises. The precedent at issue in this case was *Georgia v. Randolph*, 126 S. Ct. 1515, 164 L.. Ed. 2d 208 (2006), where the Court established the narrow exception that the consent of one occupant does not outweigh the objection of another occupant who is present on the premises. This exception was founded on social custom that a hypothetical visitor would probably not enter over the objections of a cotenant. The defendant in the present case argued that this exception still applied because he was absent only as a result of his arrest, and his objection while present should remain in effect until he "no longer wishes to keep the police out of his home."

Despite the defendant's arguments, the Court declined to consider the idea that an officer's motive in arresting an individual could invalidate otherwise reasonable searches. Therefore, the court held that "an occupant who is absent due to a lawful

detention or arrest stands in the same shoes as an occupant who is absent for any other reason." In regards to the continuing objection argument made by the defendant, the Court voiced its concern that such a rule would produce a variety of practical problems and ignore the social custom upon which *Randolph* was based. A hypothetical visitor would probably enter the premises while the objecting resident was not present, and there would be no way for the court to formulate a workable rule as to how long or under what circumstances an objection to search would be valid. In holding that the present case did not fall under the exception in *Randolph*, the Court also noted the consenting occupant's right to allow the police to search the premises if such a search is desirable to her.

Justice Ginsburg, joined by Justices Sotomayor and Kagan, wrote a dissenting opinion in the case. She disagreed with both the social and practical justifications offered by the majority. In her opinion, it was improper to draw analogies with the social custom of admitting visitors where the same social custom would never allow that visitor to conduct a search of the premises. In addition, all of the Court's practical problems concerning the circumstances and duration of an ongoing objection could have been assuaged by simply acquiring a warrant; an objection to search does not unequivocally keep the police from searching. Ginsburg notes that advances in the speed and efficiency of obtaining a warrant should keep the court from citing that difficulty as a justification for warrantless searches.

Note: In *City of Los Angeles v. Patel*, the Supreme Court held that a provision of the Los Angeles Municipal Code that requires hotel operators to make their registries available to police on demand is facially unconstitutional. 135 S. Ct. 2443 (2015). The Court emphasized the necessity of an opportunity for precompliance review and the availability of methods to preserve the quality of an administrative search. In dissent, Justice Scalia asserted that hotels fall within the category of "closely regulated" industries that may be searched without a warrant.

8. *Riley v. California*, 134 S. Ct. 2473 (2014)

In *Riley v. California*, the Supreme Court reached the question of "whether police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." The case was a consolidation of two cases raising that common question. In the first case, the defendant Riley's "smart phone" was searched without a warrant both by an officer at the scene of his arrest and an expert in gangs about two hours after his arrest. Based on photographs found on his phone, Riley was charged and convicted in connection with an earlier shooting that was unrelated to the initial crime of arrest, possession of concealed and loaded firearms. In the second case, the defendant Wurie's "flip phone" was seized at the police station after he was arrested for making an apparent drug sale. When the phone repeatedly received calls from "my house," officers opened the phone without a warrant and recovered the number associated with "my house." After searching the number in an online phone directory to obtain its address, the officers executed a search warrant on Wurie's apartment which led to the discovery

of 215 grams of crack cocaine among other contraband. He was convicted of distributing crack cocaine, possessing crack cocaine with intent to distribute, and being a felon in possession of a firearm and ammunition.

Subject to a few exceptions, the Fourth Amendment has led the Court to conclude that most warrantless searches should be considered unreasonable. In this case, Justice Roberts wrote for the Court as it decided whether warrantless cell phone searches fell under the well-established exception of a search incident to arrest. The Court began by examining the three precedents which govern such searches. First, *Chimel v. California*, 89 S. Ct. 2034, 23 L.. Ed. 2d 685 (1969), established the rule that it is reasonable to search an arrestee's person and the area within his immediate control in order to remove weapons which might endanger the officer or evidence which the arrestee might destroy. Second, the Court held in *United States v. Robinson*, 94 S. Ct. 467, 38 L. Ed. 2d 427 (1973), that no additional justification other than a lawful arrest is needed to conduct a search incident to that arrest; the reasonableness of a search does not depend upon the probability that weapons or evidence will be found on the arrestee. Lastly, in *Gant v. Arizona*, 129 S. Ct. 1710, 173 L. Ed. 2d 485 (2009), the Court emphasized the reasoning in *Chimel* and held that police could only search a vehicle when the arrestee was "unsecured and within reaching distance of the passenger compartment" unless it was "reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle."

The ruling in *Robinson* entitled an arresting officer to search the contents of a cigarette package after he removed it from the arrestee. The Court recognized that a mechanical application of this precedent would allow officers to search the contents of a cell phone, but it declined that mechanical application because it found that such a search would be viewed as fundamentally different under the twin justifications of *Chimel*. While the concerns in *Chimel* dealt with weapons or evidence to which the arrestee himself might have access, all possible dangers or evidence loss suggested by California would be the result of third party actions. Those possibilities include the pending arrival of an arrestee's confederates, remote wiping of data, and automatic encrypting of phones. The Court concluded that law enforcement is free to examine the exterior of a phone for weapons and should take advantage of existing methods of data preservation such as battery removal.

The search incident to arrest exception rests generally on heightened government interests in an arrest situation and reduced privacy interests of an arrestee. However, the Court pointed out that the reduction in privacy interests does not automatically validate any search; privacy related concerns may cause a warrant to be required if they are weighty enough. Despite the fact that the Court had upheld searches of physical items such as billfolds or address books, it declined to extend that logic because it found that a cell phone's increased storage capacity and ability to collect a pervasive variety of data led to a much greater privacy interest than a few personal items.

In anticipation that the Court would decline to extend *Robinson* to the search of a cell phone, the government put forth the following alternative rules: allowing a search when there is a reasonable belief that the phone contains evidence of the crime of arrest, restricting the scope of searches to areas where an officer might find pertinent evidence, always allowing the search of a call log, or allowing the search of data if the same information could have been obtained from a pre-digital counterpart. In short, the Court rejected all of these proposed rules because they would impose "no practical limit" or "few meaningful constraints" on officer searches. As a result of the above reasoning, the Court opted to respect the privacy of the contents of cell phones and held that "officers must generally secure a warrant before conducting such a search." In doing so, it acknowledged the impact that such a rule might have on efficient law enforcement, but the Court gave greater weight to the tradition and history of the warrant requirement than it did to the efficiency of law enforcement.

Implications:
In order to ensure the admissibility of important evidence, law enforcement officers must obtain a warrant before searching the contents of a cell phone; such a search does not fall under the exception of searches incident to a lawful arrest. The court noted that exigent circumstances might nullify this requirement, but its examples involved the extreme cases of impending terrorist activity or ongoing child abduction.

C. Driver's Privacy Protection Act of 1994

1. *Maracich v. Spears*, 133 S. Ct. 2191 (2013) involves application of the litigation exception for nondisclosure of information in the Drivers Protection Act.

The Driver's Privacy Protection Act of 1994 (DPPA), 18 U.S.C. §§ 2721–2725, regulates the disclosure and use of personal information contained in the records of state motor-vehicle departments. The statute prohibits obtaining or using personal information in driving records for the purpose of bulk marketing or solicitations without the express consent of the individuals whose information is being used. The statute does, however, permit disclosure without consent of personal information for "use in connection with any civil ... proceeding," including "investigation in anticipation of litigation." 18 U.S.C. § 2721(b)(4).

The issue before the Court in *Maracich* was whether the litigation exception to nondisclosure in Driver's Privacy Protection Act of 1994 (DPPA) covers lawyers who obtain protected personal information from driving records solely to find clients for a lawsuit. The Court answered this question in the negative.

The Respondents in *Maracich* are lawyers who filed a representative action in South Carolina state court against local car dealers, alleging that the dealers had

improperly charged certain fees to customers. Before filing suit, respondents had submitted several state Freedom of Information Act requests to the South Carolina Division of Motor Vehicles (DMV) seeking the names and addresses of thousands of individuals in order to solicit clients for a lawsuit they had pending against local car dealers. Using the information provided by the DMV, the respondent lawyers sent over 34,000 car purchase letters, which were headed "Advertising Material," which explained the lawsuit against the dealers and asked the recipients whether they wanted to participate in the lawsuit. Some car-buyers responded by suing the respondent lawyers in federal district court, alleging that the solicitations violated the DPPA. The district court granted summary judgment in favor of the respondent lawyers. On appeal, the U.S. Court of Appeals for the Fourth Circuit affirmed, concluding that the solicitations were permissible under the DPPA's litigation exception and were "inextricably intertwined" with the original lawsuit. The DPPA exception in issue allows the disclosure of personal information "for use in connection with any civil, criminal, administrative, or arbitral proceeding," including "investigation in anticipation of litigation." 18 U. S. C. §2721(b)(4). The district court granted summary judgment in favor of the respondent lawyers, holding their letters were not solicitations and that the use of information fell within the litigation exception in subsection (b)(4). The Fourth Circuit affirmed, concluding that the letters were solicitation, but that the solicitation was intertwined with conduct that satisfied the (b)(4) exception. The car buyers appealed this decision to the United States Supreme Court, which took the appeal to resolve a conflict between the Circuit Courts of Appeal. The Fourth Circuit's decision in *Maracich* conflicts with decisions of the U.S. Court of Appeals for the Third Circuit and the District of Columbia Courts of Appeals (the highest court for D.C.). On June 17, 2013, the Supreme Court reversed the Fourth Circuit Court of Appeals holding that an attorney's solicitation of clients is not a permissible purpose covered by the subsection (b)(4) litigation exception.

Note: *McDonough v. Anoka Cty.*, 799 F.3d 731 (8th Cir. 2015) (DPPA violation occurs even when improperly obtained information is never "used").

Implication:
In responding to a request for information made under the State Freedom of Information Act, W. Va. Code § 29B-1-1 *et seq.*, agencies need to be aware of and comply with exemptions from disclosure provided in W. Va. Code § 29B-1-4 and in applicable federal statutes such as the DPPA.

D. Fair Credit Reporting Act

1. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, L. Ed. 2d 635 (2016)

In Spokeo, Inc. v. Robins, the Supreme Court vacated and remanded a Ninth Circuit decision that found a plaintiff to have standing to bring suit for privacy violations where no injury occurred. Robins filed a class-action suit against Spokeo, which operated a "people search engine" for, among other users,

prospective employers, after discovering that his profile contained inaccurate information. The Ninth Circuit reversed the District Court's dismissal for failing to plead injury in fact because Spokeo had violated Robins' statutory rights under the FRCA. The Supreme Court held in the context of a FRCA claim that the injury-in-fact requirement for standing required a concrete and particularized injury. The Supreme Court explained that "[i]njury in fact is a constitutional requirement, and it is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue a plaintiff who would not otherwise have standing." In Spokeo, the injury-in-fact requirement necessitates a showing that the plaintiff suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical" (internal citing reference omitted). Because the Ninth Circuit "failed to fully appreciate the distinction between concreteness and particularization," the Supreme Court found its standing analysis to be incomplete. The Supreme Court also reiterated that a "concrete" injury need not be a "tangible" injury. The case was remanded to the Ninth Circuit solely based on the standing analysis; the Supreme Court did not rule on whether Robins had adequately alleged injury in fact. This case is still pending in the Ninth Circuit on remand.

Implication:

The implications of this case are potentially widespread. If no injury is required, multiple suits could be brought for violations of privacy. "Spokeo's challenge has drawn support from several high-profile backers, including Facebook Inc., eBay Inc., Google Inc. and Yahoo Inc., which filed an amicus curiae brief in June arguing that letting the Ninth Circuit's ruling stand would open the floodgates for a barrage of "no injury" class actions under the Telephone Consumer Protection Act, the Video Privacy Protection Act and similar statutes." Allison Grande, Privacy Cases to Watch in 2015, Law360 (Jan. 2, 2015, 3:26 p.m.). Although the Supreme Court criticized the Ninth Circuit's standing analysis, the ultimate outcome of the case remains uncertain.

3.0 West Virginia

3.1. Executive Order No. 6-06 (August 16, 2006)

Description:

Executive Order No. 6-06 rescinds and supersedes Executive Order No. 7-03. Order 6-06 designates the Chairperson of the Health Care Authority (HCA) as the person responsible for protecting the privacy of confidential and personally identifiable information collected and maintained by Executive Branch Departments. The Chief Technology Officer (CTO) is responsible for the information security of the Executive Branch Departments.

The HCA Chair is empowered to develop a privacy program, create and maintain a privacy team, issue privacy policies, develop and implement data classification schemes, and develop measures to remediate, as appropriate, following privacy audits.

The CTO is to create an information security team to oversee the development and supervision of security policies, data classification schemes, and measures to remediate, as appropriate, following security audits.

Implications:

- An Executive Branch Privacy Management Team, chaired by the HCA, is created with representation from each Department. Each Executive Branch Department must designate a Privacy Officer who shall actively participate on the Team.
- The Team shall raise privacy awareness, perform privacy assessments, determine privacy requirements, and implement appropriate policies and procedures.
- The Team shall look for opportunities to improve the protection of private information, including:
    - Restricting disclosure of personal information;
    - Increasing individual access to personal information;
    - Granting individuals the right to seek amendment of personal information;
    - Establishing a State government policy for the collection, maintenance and dissemination of personal information; and,
    - Complying with privacy laws, including HIPAA and other federal and State mandates.

Source:

Exec. Order No. 6-06 (August 16, 2006)
http://www.privacy.wv.gov/SiteCollectionDocuments/Executive%20Order%206-06.pdf

Principles:

Accountability, Minimum Necessary and Limited Use, Individual Rights, Security Safeguards

3.2. Freedom of Information Act

W. Va. Code § 29B-1-1 *et seq*.

Description:

The State Freedom of Information Act ("FOIA"), W. Va. Code § 29B-1-1 *et seq*., like the Federal FOIA, mandates that "[e]very person has a right to inspect and copy any public record of a public body in this State, except as otherwise" exempted.

The Legislature exempts "[i]nformation of a personal nature such as that kept in a personal, medical or similar file, if the public disclosure thereof would constitute an unreasonable invasion of privacy, unless the public interest by clear and convincing evidence requires disclosure in the particular instance." An individual can always inspect and copy his or her own records.

Additionally, information may be specifically exempted from disclosure by another statute; *see e.g.,* discussion regarding the Records Management and Preservation of Essential Records Act which protects certain PII. Also exempted from FOIA disclosure are computing, telecommunications, and network security records, passwords, security codes, or programs used to respond to or plan against acts of terrorism which may be the subject of a terrorist act. Information relating to the design of corrections and jail facilities and policies and procedures relating to the safe and secure management of inmates are also exempted, along with design facilities and the Division of Juvenile Services.

In 2015, House Bill 2636 was passed amending the State FOIA amending W. Va. Code § 29B-1-1 *et seq.* The bill also added another exemption; information contained in a concealed weapon permit by amending W. Va. Code § 29B-1-4. Importantly, the term 'public record' was redefined and expanded to "any writing containing information prepared or received by a public body, the content or context of which, judged either by content or context, relates to the conduct of the public's business." Additionally, § 29B-1-3a was added to the code, requiring every public body that receives a FOIA request to inform the Secretary of State of the request along with at least: (1) the nature of the request; (2) the nature of the public body's response; (3) time-frame required to comply with the response; and (4) the amount of reimbursement charged to the person that submitted the FOIA request. H.B. 2636 amended § 29B-1-3 regarding fees that can be charged for FOIA requests, requiring that the reasonable fee charged cannot "charge a search or retrieval fee or otherwise seek reimbursement based on a man-hour basis as part of costs associated with making reproduction of records." Finally, the Secretary of State must maintain an electronic database of all FOIA requests.

In 2016, House Bill 2800 was passed amending §§ 29B-2-2 and -4 to add the contact information of law enforcement officers and the names of their family members to the list of exemptions from public records requests.

As of 2016, there are a total of twenty-one exemptions from disclosure under the Act which may be asserted by an agency.

There is a private right of action for violations of the Act, and courts may award criminal penalties and attorney fees and costs for such violations.

Implications:

- Departments shall ensure that their responses to FOIA requests do not include PII or medical information that is exempt from FOIA.
- Departments shall ensure that their responses to FOIA do not include any other exempted or confidential information, without the approval of their Department head. *See* West Virginia Privacy Case Law.
- Departments shall inform the Secretary of State of any and all State FOIA requests with at least the minimum information required by statute.
- Departments must charge a reasonable fee, but cannot charge based on man-hours required to comply with a request.
- *See* 5.0 West Virginia Privacy Case Law

Source:

W. Va. Code §§ 29B-1-1 to -7 – West Virginia Freedom of Information Act
http://www.legis.state.wv.us/wvcode/ChapterEntire.cfm?chap=29b

West Virginia House Bill 2636
http://www.legis.state.wv.us/Bill_Status/bills_text.cfm?billdoc=HB2636 SUB ENR.htm&yr=2015&sesstype=RS&i=2636

West Virginia House Bill 2800
http://www.legis.state.wv.us/Bill_Status/bills_text.cfm?billdoc=HB2800 SUB ENR.htm&yr=2016&sesstype=RS&i=2800

U.S. Department of Justice Guide to the Freedom of Information Act (2016)
http://www.justice.gov/oip/foia-guide.html

Principles:

Individual Rights and Individual Participation, Security Safeguards, Minimum Necessary and Limited Use

3.3. Records Management and Preservation of Essential Records Act

W. Va. Code §§ 5A-8-5, -20, -21, -22

Description:

West Virginia law requires State government to safeguard certain personally identifying information with respect to State employees and citizens and to disclose to non-governmental entities only as authorized by law. With regard to State officers, employees, retirees, or the legal dependents thereof, the following individual identifiers are confidential and exempt from disclosure: home address, SSN, credit or debit card numbers, driver's license number, and marital status or maiden name. With regard to individuals generally, Social Security Numbers and credit or debit card numbers are confidential and exempt from disclosure.
W. Va. C.S.R. § 143-1-20 reads:

"The business of the Division of Personnel shall be conducted in such a manner as to ensure the privacy rights of all applicants and employees, in accordance with W. Va. Code §§ 29B-1-1 *et seq*., the State Freedom of Information Act and 5A-8-1 *et seq*., the Public Records Management and Preservation Act. Examination scoring keys, applicant and employee residential addresses and phone numbers, applicant and employee medical information, and other information which the Director may deem confidential shall be maintained under strictest confidentiality and released only upon proper written authorization of the applicant or employee or by order of a court of competent jurisdiction."

"State record" is defined to mean an electronic record created and maintained by state agencies. The State government must establish and apply efficient methods to the creation, utilization, maintenance, retention, preservation, and disposal of state records.

In 2013, W. Va. Code § 5A-8-20 (alternate storage of state records) was amended by H. B. 2968 to authorize the use of an additional medium in archiving records. The bill sets forth standards the additional medium must meet and requires the state records administrator to establish a procedure for executive agencies to follow. Consistent with the State Constitution, the bill permits each house of the Legislature to determine on its own or jointly the procedure for the storage of legislative records. The bill permits any person or entity to purchase one copy of any archived or preserved state record.

Implications:

- Departments must establish procedures to ensure that identifiers are safeguarded and kept confidential.
- Departments must establish procedures to ensure that personal identifiers are protected from disclosure to non-governmental entities, unless the disclosure is authorized by law. Procedures regarding FOIA should be reviewed to ensure conformance with these laws.

- Departments must establish policies and procedures governing record retention and disposal of varying types of state records as permitted by applicable law.

Source:

W. Va. Code § 5A-8-3 – Definitions
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=8&section=3#08

W. Va. Code § 5A-8-5 – State records administrator
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=8&section=5#08

W. Va. Code § 5A-8-20 – Alternate storage of state records
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=8&section=20#08

W. Va. Code § 5A-8-21 – Limitation on release of certain personal information maintained by state agencies and entities regarding state employees
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=8&section=21#08

W. Va. Code § 5A-8-22 – Personal information maintained by state entities
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=8&section=22#08

Principles:

Minimum Necessary and Limited Use, Security Safeguards, Accountability

3.4. Information Services and Communications Division

W. Va. Code §§ 5A-7-1, -2, and -11

Description:

The Information Services and Communications Division of the Department of Administration establishes, develops, and improves data processing and telecommunication functions in the various Departments and promulgates standards in the utilization of data processing and telecommunication equipment.

Article 7 creates a specific privacy and security obligation:

"Under no circumstances shall the head of any department or agency deliver to the [Information Services and Communications] Division any records required by law to be kept confidential, but such head may extract information from such records for data processing by the division, provided the integrity of such confidential records is fully protected."

Implications:

- Departments must develop protocols for removing confidential, personal, or identifiable health information prior to delivering requested data to the division.

Source:

W. Va. Code § 5A-7-2 – Division created; purpose; use of facilities; rules and regulations
http://www.legis.state.wv.us/wvcode/ChapterEntire.cfm?chap=05a&art=7&section=2#07

W. Va. Code § 5A-7-1 – Definitions
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=7&section=1#07

W. Va. Code § 5A-7-11 – Confidential records
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=7&section=11#07

Principles:

Minimum Necessary and Limited Use, Security Safeguards

3.5. The Uniform Electronic Transactions Act

W. Va. Code § 39A-1-1 *et seq*.
W. Va. C.S.R. § 153-30

Description:

The Uniform Electronic Transactions Act applies to transactions between parties where both have agreed to use electronic records and signatures. Whether the parties have agreed to use electronic transactions is determined from the context and surrounding circumstances, including the parties' conduct. "Transaction" means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs. The Act creates a duty to give notice in certain circumstances. The Act does not apply to wills and other testamentary writings; court orders; most U.C.C. transactions; cancellation or termination of health insurance, health benefits, or life insurance benefits (excluding annuities); recall of a product; material failure of a product that risks endangering health or safety; or any document required to accompany any transportation or handling of hazardous materials, pesticides, or other dangerous materials.

If a statute, regulation or other rule of law requires that information relating to a transaction be provided or made available to a consumer in writing, the use of an electronic record to provide or make available such information satisfies the requirement that such information be in writing if the consumer has affirmatively consented to such use and the consumer, prior to consenting, has been provided clear notice which states the following:

1. The consumer's right or option to have the record provided or made available on paper or in non-electronic form;
2. The right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any consequences, which may include termination of the parties' relationship, or fees in the event of such withdrawal;
3. Whether consent applies to a particular transaction or category of records;
4. How the consumer can withdraw consent; and
5. How the consumer may obtain a paper copy and a description of the fees, if any, for the paper copy.

Prior to consenting, the consumer must be provided with a statement of the hardware and software requirements for access to and retention of the electronic records, and he or she must consent electronically in a manner that demonstrates the consumer can access relevant information in electronic form. Once consent has been given, the consumer must be notified if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent.

The statute also authorizes that where the law requires a record to be retained, the requirement is satisfied by retaining an electronic record of the information in the original record that (1) accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record and (2) remains accessible for later reference. If the law requires retention of a check, that requirement can be satisfied electronically.

Implications:

- Departments engaging in transactions with the public must develop appropriate notice and consent documents upon moving to electronic transactions.
- Departments must develop a method to store the consent or withdrawal of consent documents.

Source:

W. Va. Code § 39A-2-1 *et seq*. – Uniform Electronic Transactions Act
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=39a&art=1

W. Va. Code § 39A-2-1 *et seq*. – Consumer Protections and Responsibilities In Electronic Transactions
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=39a&art=2

W. Va. Code § 39A-3-1 *et seq.* – Digital Signatures; State Electronic Records and Transactions
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=39a&art=3

W. Va. C.S.R. § 153-30 – Use Of Digital Signatures, State Certificate Authority And State Repository
https://apps.sos.wv.gov/adlaw/csr/readfile.aspx?DocId=19889&Format=PDF

Principles:

Notice, Consent, Individual Rights

3.6. State Health Privacy Laws

Description:

The West Virginia Code is a patchwork quilt of provisions governing the confidentiality of health related information. The HIPAA preemption analysis on the State Privacy Office website references and summarizes the health-related confidentiality laws.

Implications:

- Departments collecting, using or disclosing health related information must ensure that they have procedures in place to carry out the mandated confidentiality and other privacy aspects.
- Departments collecting, using, or disclosing health related information in conjunction with third parties must have Business Associate Agreements.

Source:

West Virginia State Privacy Office, Health Care Authority –West Virginia Health Care Privacy Laws and HIPAA Preemption Analysis
http://www.privacy.wv.gov/HIPAA/Pages/default.aspx

Principles:

Consent, Individual Rights, Minimum Necessary and Limited Use, Security Safeguards, Accountability

3.7. West Virginia Health Information Network

W. Va. Code § 16-29G-1 *et seq*.
W. Va. C.S.R. § 65-28

Description:

The West Virginia Health Information Network (WVHIN), under the oversight of the West Virginia Health Care Authority, was created to promote the design, implementation, operation and maintenance of a fully interoperable statewide network to facilitate public and private use of health care information in the State. As part of its duties, the Health Care Authority "shall ensure" that patient-specific protected health information be disclosed only in accordance with the patient's authorization or best interest to those having a need to know in compliance with State confidentiality laws, the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The health information, data, and records of the WVHIN shall be exempt from disclosure under FOIA.

In its legislative rule establishing the standards for the development, implementation, and operation of the WVHIN, which went into effect May 18, 2014, the Health Care Authority defined participating organizations as Covered Entities, Business Associates, or public health agencies that have been approved by the WVHIN. Participating organizations must designate authorized users who are their only employees that may access the WVHIN. The rule provides for two types of protected health information transactions: an inquiry by a participating organization for treatment purposes or a point-to-point disclosure between two participating organizations. Both types of transaction must designate the permissible purpose of the disclosure and use, such as treatment, emergency treatment, or public health reporting. Disclosures and uses should comply with the "minimum necessary" standard of the HIPAA Privacy Rule.

Participating Organizations must also provide a written notice, developed by the WVHIN, which affords first time patients the opportunity to make an informed decision on whether to opt-out of inclusion in the WVHIN. Patients are considered active participants in the information exchange unless they elect to opt-out in a patient encounter or online; patients may revoke a decision to opt-out at any time. Even when opted out, the WVHIN will still disclose protected health information to state or federal agencies for the purpose of public health reporting.

Implications:

- Departments and participants in the WVHIN must work with the Authority to protect the privacy of patient-specific health information.
- Departments and private participants should be familiar with the permissible disclosures and uses of protected health information and adhere to the "minimum necessary" standard of HIPAA when contemplating disclosures through the WVHIN's Health Information Exchange.

- Authorized users of the WVHIN must be designated, and no unauthorized user may be given access to the WVHIN for any reason.
- Site administrators must be selected who will be the primary point of contact with the WVHIN.
- Participating organizations must promptly report to the WVHIN when malfunction, misuse, or breach of the health information exchange occurs.
- Participating organizations must identify, classify, segregate, and block the disclosure of sensitive health information (such as mental health, drug or alcohol abuse, and patient restricted information) within its records.
- State and federal agencies can obtain protected health information from the exchange for purposes of public health reporting regardless of whether an individual has decided to opt-out.

Source:

W. Va. Code § 16-29G-1 *et seq*. – West Virginia Health Information Network
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=16&art=29G

W. Va. C.S.R. § 65-28 – West Virginia Health Information Network Rule
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=9128

Principles:

Accountability, Consent, Individual Rights, Minimum Necessary and Limited Use, Security Safeguards

3.8. Maxwell Governmental Access to Financial Records Act

W. Va. Code § 31A-2A-1 *et seq*.

Description:

This law sets forth the conditions under which a financial institution (bank, savings and loan association, trust company, or credit union) may disclose a customer's financial records to a State entity, and the conditions under which a State entity may have access to or obtain those records. Examples of appropriate access include customer authorization, legal process, law enforcement resulting from a criminal investigation, and requirement or permission by any other State or federal law. A State entity that receives information in accordance with the procedure set forth in the Act may not disclose financial records to any other State entity or any other person unless the receiving State entity or other person is authorized by law or by the customer to receive the records. This law, however, does not prevent a receiving State entity from disclosing properly obtained financial records "to facilitate a lawful proceeding, investigation, examination or inspection by a state entity." Financial institutions are required to obtain written certification from the receiving State entity that it has complied with the applicable provisions of this law. A financial institution may disclose or produce financial records to a state entity in compliance with a subpoena if the subpoena contains a certification that a copy of the subpoena was served on the customer at least 10 days prior to the date of production or that service on the customer has been waived for good cause by the Circuit Court of Kanawha County or another circuit court of competent jurisdiction.

There are 18 exceptions to this law; examples include banking and insurance regulatory activities and various disclosures to DHHR regarding eligibility for public assistance and the federal parent locator service.

There are criminal and civil penalties for violations of this law. There is also a private right of action.

Implications:

- Departments that have financial institution operations shall ensure that they have policies and procedures governing the disclosure of customer financial records to any State entities.
- Departments that obtain customers' financial records shall ensure that they have policies and procedures regarding disclosure of the records.

Source:

W. Va. Code § 31A-2A-1 *et seq*. – Maxwell Governmental Access to Financial Records Act
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=31a&art=2A

Principles:

Consent, Minimum Necessary and Limited Use

3.9. Confidentiality and Disclosure of Tax Returns and Return Information

W. Va. Code §§ 11-10-5d, -5s, -5u, -5v, -5w, -5y, 11-13J-10, -13Q-20, -13R-11, -13S-10, -13U-8, -13AA-9, -13BB-11.
W. Va. C.S.R. §§ 110-50A-1, -50B-1, -50D-1, -50E-1, -50F-1 and -50G-1

Description:

With certain enumerated exceptions, tax returns, associated reports and declarations, and the information they contain are confidential and may not be disclosed to anyone. This law governs both the Tax Department's disclosure of return information and State government in general. Except for very specific situations, such as under a court order, the release of confidential information is at the discretion of the Tax Commissioner. Departments receiving return information will be required to enter into an exchange of information agreement with the Tax Department, and they must safeguard the information as confidential. Tax return information is not subject to FOIA.

Disclosure may occur:

- When required by the Tax Commissioner in an official investigation.
- Where the Tax Commissioner is a party in a proceeding to determine the amount of tax due.
- When the taxpayer authorizes disclosure to an individual.
- For use in criminal investigations.
- To a person having a material interest, as defined by the Tax Commissioner in regulations.
- For statistical use.
- Regarding disclosure of the amount of an outstanding lien on property to such person who has a right in the property or intends to obtain a right.
- For reciprocal exchange in the administration of tax programs.
- In administrative decisions (Identifying characteristics or facts about the taxpayer shall be omitted or modified so the name or identity of the taxpayer is not disclosed).
- When the Tax Commissioner determines that certain taxpayer information (such as those who have a current business registration certificate, those who are licensed employment agencies, etc.) should be released to enhance enforcement.
- To the Bureau for Child Support Enforcement.
- For purposes of jury selection.
- As required to be disclosed by W. Va. Code § 11-10-5s.
- Regarding names of persons making retail sales of tobacco products.
- To the State Treasurer for return, recovery and disposition of unclaimed and abandoned property.
- To county assessors, the Department of Environmental Protection, and the Public Service Commission regarding certain oil and gas production information.

- To the Consolidated Pension Retirement Board.
- Regarding certain information pertaining to neighborhood investment tax credit program.
- Regarding certain information about economic opportunity tax credit.
- Regarding certain information about strategic research and development tax credit.
- Regarding certain information about manufacturing investment tax credit program.
- Regarding certain information about high-growth business investment tax credit program.
- Regarding certain information about commercial patent incentive tax credit program.
- Regarding certain information about mine safety technology tax credit program.
- To the Alcohol Beverage Control Administration.
- To the Department of Labor, the Department of Commerce, the Commissioner of Insurance, the Commissioner of Motor Vehicles, the Commissioner of Employment Programs, the Office of Governor, the Department of Transportation, and the Department of Environmental Protection.
- To the West Virginia Lottery.
- To the State Fire Marshal.
- To the State Attorney General relevant to enforcement of Tobacco Master Settlement Agreement.
- To the State Auditor for use in offset programs aimed at collecting unpaid and delinquent state taxes pursuant to a written agreement between the Tax Commissioner and the State Auditor.

There are criminal penalties for violation of this law.

The Tax Department has issued a proposed rule that parallels other existing information exchange agreements. The rule governs the exchange of information between the Tax Commissioner and Commerce Secretary, Environmental Protection Secretary, Forestry Director, and the Public Service Commission Commissioners. Currently, the rule has passed the Legislative Rule-Making Review Committee with no changes.

Implications:

- The Tax Department must ensure that it has policies in place such that tax returns and related information are only disclosed in accordance with this law.
- Departments must assess whether they receive tax return information, and if they do, they must ensure that they have policies requiring that it be held confidentially and only disclosed in accordance with this law and the terms of the exchange of information agreement signed with the Tax Department.

Source:

W. Va. Code § 11-10-5d – Confidentiality and disclosure of returns and return information
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=10&section=5D#10#10

W. Va. Code § 11-10-5s – Disclosure of certain taxpayer information
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=10&section=5S#10#10

W. Va. Code § 11-10-5u – Disclosure of persons making retail sales of tobacco products
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=10&section=5U#10#10

W. Va. Code § 11-10-5v – Disclosure of tax information to the treasurer for return, recovery and disposition of unclaimed and abandoned property
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=10&section=5V#10#10

W. Va. Code § 11-10-5w – Confidentiality and disclosure of information set forth in the oil and gas combined reporting form specified in subsection (d), section three-a, article thirteen- a of this chapter to county assessors, the Department of Environmental Protection and to the Public Service Commission; offenses; penalties
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=10&section=5W#10#10

W. Va. Code § 11-10-5y – Disclosure of return information to Consolidated Public Retirement Board
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=10&section=5Y#10#10

W. Va. Code § 11-13J-10 – Public information relating to tax credit
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=13J&section=10#13J#13J

W. Va. Code § 11-13Q-20 – Tax credit review and accountability
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=13Q&section=20#13Q#13Q

W. Va. Code § 11-13R-11 – Tax credit review and accountability
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=13R&section=11#13R#13R

W. Va. Code § 11-13S-10 – Tax credit review and accountability

http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=13S&section=10#13S#13S

W. Va. Code § 11-13U-8 – Tax credit review and accountability
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=13U&section=8#13U#13U

W. Va. Code § 11-13AA-9 – Tax credit review and accountability
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=13AA&section=9#13AA#13AA

W. Va. Code § 11-13BB-11 – Tax credit review and accountability
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=11&art=13BB&section=11#13BB#13BB

W. Va. C.S.R. § 110-50A-1 – Exchange of Information Agreement Between Tax Division and Division of Environmental Protection,
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=7904

W. Va. C.S.R. § 110-50B-1 – Exchange of Information Agreement Between the State Tax Division and the Alcohol Beverage Control Administration,
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=7905

W. Va. C.S.R. § 110-50D-1 – Exchange of Information Agreement Between Commissioner And Labor, Insurance Commission, Motor Vehicles, Bureau of Employment Programs and Governor
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=7906

W. Va. C.S.R. § 110-50E-1 – Exchange of Information Agreement Between the State Tax Department and the West Virginia Lottery
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=7907

W. Va. C.S.R. § 110-50F-1 – Exchange of Information Agreement between the State Tax Department and the Office of the State Fire Marshal
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=7909

W. Va. C.S.R. § 110-50G-1 – Exchange of Information Agreement Between the State Tax Department and the Department of Commerce, the Department of Transportation and the Department of Environmental Protection
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=7910

W. Va. C.S.R. § 110-50H-1 (Proposed Rule) – Exchange of Information Agreement Between the Commissioner of the Tax Division of the Department of Revenue and the Secretary of the Department of Commerce, The Secretary of the Department of Environmental Protection, the Director of the Division of Forestry of the

Department of Commerce, and the Commissioners of the Public Service Commission
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=9863
Principles:
Consent, Minimum Necessary and Limited Use, Security Safeguards

3.10. Uniform Motor Vehicle Records Disclosure Act

W. Va. Code §§ 17A-2A-1 to -14, 17B-2-12a
W. Va. C.S.R. § 91-08

Description:

This law implements the federal Driver's Privacy Protection Act of 1994 to protect individual privacy by limiting the use and disclosure of personal information in connection with motor vehicle records, except as authorized by the individual or by law. A verbal request is sufficient to disclose records that do not contain personal information. Records containing personal information must be requested in writing by a permitted user.

Note: Amendments to W. Va. Code § 17B-2-12a in 2014 allow the Commissioner of the Motor Vehicle Administration to provide a program of electronic renewal notices and an electronic web-based renewal process. Currently, the DMV website only allows drivers to request their driving record, pay fees for driver's license reinstatement, and renew registration. The Administration will need to cautiously ensure the electronic security of personal information in connection with motor vehicle records as it moves forward with electronic functions.

Implications:

- The DMV must have procedures to ensure that personal information obtained in connection with the motor vehicle record is only used and disclosed as authorized by law or with the consent of the individual.
- Departments must assess whether they obtain personal information from the DMV.
- Departments obtaining personal information from the DMV must ensure that they have procedures detailing use and disclosure of the personal information, as well as record keeping requirements. Note: State law requires an individual's express consent for re-disclosure.

Source:

W. Va. Code §§ 17A-2A-1 to -14 – Uniform Motor Vehicle Records Disclosure Act
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=17a&art=2A

W. Va. Code § 17B-2-12a – Renewal of driver's license upon expiration; vision screening; renewal fees
http://www.legis.state.wv.us/Bill_Status/bills_text.cfm?billdoc=SB431%20SUB2%20ENR.htm&yr=2014&sesstype=RS&i=431

W. Va. C.S.R.. § 91-08 – Disclosure of Information from the Files of the Division of Motor Vehicles
https://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=5897

W. Va. DMV Online Services
https://apps.wv.gov/dmv/selfservice

Principles:
Consent, Minimum Necessary and Limited Use, Security Safeguards

3.11. Consumer Credit and Protection Act, General Consumer Protection

W. Va. Code § 46A-6-101 *et seq.*
W. Va. C.S.R. § 106-01

Description:

This law prohibits "[u]nfair methods of competition and unfair or deceptive trade practices" and is similar to Section 5 of the Federal Trade Commission Act ("FTCA") which gives the FTC the power to enforce promises made in privacy notices, as well as challenge unfair information practices which result in substantial injury to consumers.
https://www.ftc.gov/tips-advice/business-center/privacy-and-security
In 2015, West Virginia passed Senate Bill No. 315, which amends W. Va. Code § 46A-6-101 to reflect the intent of the legislature that courts be guided by the FTCA Section 5 as well as the FTC and federal courts' interpretation of that section.

There is a private right of action.

Implications:

- Departments must accurately represent privacy policies in privacy notices.
- Departments must comply with promises made in privacy notices.
- Departments cannot put consumers at risk without an offsetting benefit. For example, if a company collects PII without reasonable security measures and does not tell the consumers, it would constitute an unfair trade practice.
- Departments cannot retroactively materially change a privacy notice with respect to information already collected without express, affirmative, opt-in authorization.

Source:

W. Va. Code § 46A-6-101 et seq. – West Virginia Consumer Credit and Protection Act, General Consumer Protection
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=46a&art=6

Senate Bill 315
http://www.legis.state.wv.us/Bill_Status/bills_text.cfm?billdoc=sb315%20intr.htm&yr=2015&sesstype=RS&i=315

W. Va. C.S.R. § 106-01 – Regulations Pertaining to WV Consumer Credit and Protection Act
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=872

Principles:

Notice, Consent, Minimum Necessary and Limited Use

3.12. Computer Crime and Abuse Act

W. Va. Code §§ 61-3C-1 *et seq*., -8A-1 *et seq.*

Description:

The Computer Crime and Abuse Act defines crimes for misuse and abuse of computers and computer data. The Legislature specifically recognizes the public's "privacy interest" in being protected from computer abuse. The Act specifically applies to the State and its subdivisions; it provides a private right of action which may include a claim for punitive damages. There are numerous crimes delineated in the statute which are either felonies or misdemeanors depending on the monetary value of the crime. Examples of the delineated crimes are as follows:

- Willful disruption of computer services or willful denial of computer services to an authorized user is a misdemeanor.
- Knowing and willful access of any computer to execute any scheme to defraud or obtain money by fraudulent pretenses is a felony.
- Knowing and willful access of any computer to obtain services without an authorization to do so is a misdemeanor.
- Willfully obtaining, without authorization, confidential information is a misdemeanor
- Obtaining employment and salary information or other personal information is a misdemeanor.
- Interruption or impairment of the provision of medical services or other services provided by any State agency is a felony.

Implications:

- Departments need to develop policies and procedures to ensure, to the extent possible, that their employees are in strict conformance with the appropriate and authorized uses for the State's computers and software.
- The Department of Administration should check with the Board of Risk and Insurance Management ("BRIM") that there is coverage for civil suits brought against the State or its employees under this Act.

Source:

W. Va. Code § 61-3C-1 *et seq*. – West Virginia Computer Crime and Abuse Act
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=61&art=3C

W. Va. Code § 61-8A-1 *et seq.* – Preparation, Distribution or Exhibition of Obscene Matter To Minors (*See* § 61-8A-1 defining "computer" and "computer network")
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=61&art=8A

Principles:

Minimum Necessary and Limited Use, Security Safeguards

3.13. Bureau for Child Support Enforcement, Confidentiality

W. Va. Code §§ 48-18-122, -131
W. Va. C.S.R. § 97-01

Description:

All child support records are confidential and protected from release except as otherwise provided by law. Unless the person gives permission, only a court of competent jurisdiction, a state agency with an appropriate cooperative agreement, a foreign child support agency, or prosecutor pursuing criminal action directly arising from non-payment may obtain confidential records. In addition, the Bureau for Child Support Enforcement maintains a Central State Case Registry for child support orders, which is subject to privacy and confidentiality safeguards at both the state and federal level. Information may be shared among designated agencies to determine child support amounts or assist with enforcement of support orders.

It is a misdemeanor to violate the confidentiality provisions.

Implications:

- Departments must adopt policies to safeguard their employees' child support orders.
- Departments should understand whether they have cooperative agreements in place with the Bureau for Child Support Enforcement.

Source:

W. Va. Code § 48-18-122 – Central state case registry
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=48&art=18&section=122#18

W. Va. Code § 48-18-131 – Access to records, confidentiality
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=48&art=18&section=131#18

W. Va. C.S.R. § 97-01 – General Procedures Pertaining to Documents and Files
https://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=9174

Principles:

Minimum Necessary and Limited Use, Security Safeguards

3.14. Sharing of Domestic Violence Information

W. Va. Code §§ 48-27-206, -802; 51-1-21

Description:

This law, coupled with the repeal of § 48-27-803, permits the following agencies to report domestic violence information to the West Virginia Criminal Identification Bureau, the West Virginia Domestic Violence Database, and other entities as permitted or required by law:

- West Virginia state police, county sheriffs and deputies, and municipal police departments;
- The Department of Health and Human Resources;
- Any other state agency that receives reports of child abuse not reported elsewhere; and
- Any federal agency whose purpose includes enforcement, maintenance, and gathering of criminal and civil records relating to federal domestic law.

Implications:

- Departments will update policies to permit the reporting of domestic violence information to the appropriate entities as permitted or required by law.

Source:

Prevention and Treatment of Domestic Violence
W. Va. Code § 48-27-206 – Law-enforcement agency defined
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=48&art=27&section=206#27#27

W. Va. Code § 48-27-802 – Maintenance of Registry by State Police.
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=48&art=27&section=802#27#27

Supreme Court of Appeals of West Virginia
W. Va. Code § 51-1-21 – Authority to maintain domestic violence database.
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=51&art=1&section=21#01

Domestic Violence, Sexual Assault, and Stalking Data Resource Center (no longer updated)
http://www.jrsa.org/dvsa-drc/index.html

Principles

Minimum Necessary Limited Use, Notice, Accountability

3.15. The Emergency Medical Services Act

W. Va. Code § 16-4C-1 *et seq*.
W. Va. C.S.R.§§ 64-27-1 *et seq*.,64-48-1 *et seq.*

Description:

The Emergency Medical Services Act, W. Va. Code § 16-4C-1 *et seq.*, establishes the Office of Emergency Medical Services under the Bureau for Public Health. The related rule, W. Va. C.S.R. § 64-27, requires the Office of Emergency Medical Services to "ensure the security and confidentiality of protected information within the Trauma and Emergency Medical Information System according to State and federal guidelines."

In addition, according to W. Va. C.S.R. § 64-48, regulations may be imposed setting forth the requisite standards and requirements for certification or recertification of Emergency Medical Service personnel, as well as the requirements that ambulance operators must meet. Upon submission of an application for these positions, background checks may be required, and the results of those background checks will not be released.

Implications:

- Departments must work with the Agency to ensure confidentiality within the framework of an emergency.
- Departments should continue to monitor the implementation of pertinent regulations and confirm they are in compliance as to what types of information must be maintained as confidential.

Source:

W. Va. Code § 16-4C-1 *et seq*. – Emergency Medical Services Act
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=16&art=4C

W. Va. C.S.R. § 64-27 – Statewide Trauma/Emergency Care System
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=9541

W. Va. C.S.R. § 64-48 – Emergency Medical Services
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=9885

Principles:

Minimum Necessary and Limited Use, Security Safeguards

3.16. Insurance Commissioner Rule, "Privacy of Consumer Financial and Health Information"

W. Va. Code § 33-6F-1
W. Va. C.S.R. §§ 114-57-1 *et seq*., 114-62-1 *et seq*.

Description:

These privacy rules of the West Virginia Insurance Commissioner apply to all licensed insurers, producers, and other persons licensed or registered pursuant to Chapter 33 of the West Virginia Code. While this rule does not apply to State entities such as BRIM or PEIA, it does apply to insurance licensees who have contracted with the State to provide services. "Nonpublic personal information" is defined to include nonpublic personal financial information and nonpublic personal health information. Licensees must provide annual disclosure notices to consumers of the privacy notices and practices. A licensee may not disclose personal financial information to nonaffiliated third parties unless otherwise permitted by the law or rule. The requirements and limitations associated with disclosures to third parties are enumerated in § 114-57-9 of the Code of State Rules. A licensee who must comply with HIPAA is deemed to comply with the provisions governing privacy of health information; otherwise licensees must maintain the confidentiality of health information and obtain written authorization prior to disclosing personal health information, which authorization can be electronic.

In addition, in accordance with the Gramm-Leach-Bliley Act, the Insurance Commissioner has developed rules for safeguarding customer information, which is detailed in title 114, series 62 of the Code of State Rules. Each licensee must have a written information security program. Nonpublic personal information, whether in paper or electronic format, is covered by this rule.

Implications:

- These rules apply to licensed insurers utilized by agencies.

Source:

W. Va. Code § 33-6F-1, *et seq.* – Disclosure of Nonpublic Personal Information
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=33&art=6F

W. Va. C.S.R.. § 114-57 – Privacy of Consumer Financial and Health Information
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=3461

W. Va. C.S.R.. § 114-62 – Standards for Safeguarding Consumer Information
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=3467

Principles:

Security Safeguards, Consent

3.16.1. External Review of Issuers' Adverse Health Insurance Determinations

W. Va. C.S.R. §§ 114-95-1 *et seq*., 114-96-1 *et seq.*, 114-97-1 *et seq.*

Description:

The Insurance Commissioner has promulgated three new rules which went into effect on July 6, 2014. Rules 114-95 and 114-96 have to do with establishing proper procedures for utilization review, benefit determination, and internal grievances with regards to issuers.

Rule 114-97 allows for the external review of adverse determinations if the internal grievance procedure of an issuer has been exhausted or if an expedited review is appropriate because of the covered person's health. When noticing an adverse determination, issuers are required to give notice to covered persons of their right within four months to make a written request to the Insurance Commissioner for an external review. That notice must include a form approved by the Commissioner by which the covered person authorizes the disclosure of his or her PHI for purposes of the external review. Based on information from the issuer and covered person, the Commissioner may decide to assign the determination to a random Independent Review Organization (IRO) which has been approved by the Commissioner. In order to become approved by the Commissioner, an IRO must have a quality assurance mechanism in place which ensures the confidentiality of medical and treatment records.

Implications:

- These rules apply to licensed insurers utilized by agencies.

Source:

W. Va. C.S.R. § 114-95 – Utilization Review and Benefit Determination
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=9139

W. Va. C.S.R. § 114-96 – Health Plan Issuer Internal Grievance Procedure
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=9140

W. Va. C.S.R. § 114-97 – External Review of Adverse Health Insurance Determinations
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=9140

Principles:

Security Safeguards, Consent

3.17. All-Payer Claims Database

W. Va. Code § 33-4A-1 *et seq.*
W. Va. C.S.R. §§ 114A-01, -02

Description:

West Virginia Code § 33-4A-1, *et. seq.* provides for the creation of an all-payer claims database which collects, retains, uses, and discloses information concerning the claims and administrative expenses of health care payers. The statute requires the database to be developed by the Insurance Commissioner, the Secretary of Health and Human Resources, and the Chairperson of the Health Care Authority. It provides for the safekeeping and protection of personal identifiers and the confidentiality of information contained in the database. Under the statute, certain information provided by insurance companies to the West Virginia Insurance Commissioner is considered to be confidential and is therefore exempted from disclosure under the Freedom of Information Act. It also provides that the confidential information is not subject to subpoena or discoverable in a private civil action. Further, there are conditions under the statute relating to the Insurance Commissioner's authority to release, share and receive documents otherwise treated as confidential.

On July 1, 2012, Rule 114A-1 titled "All-Payer Claims Database – Privacy and Security Requirements" became effective. The rule requires the transmission and retention of data to be secured in a manner that prevents unauthorized access and ensures that the confidentiality, integrity, and availability of all data transmitted to the all-payer claims database is in compliance with the HIPAA Security and Privacy Rules.

Source:

W. Va. Code § 33-4A-1 *et seq.* – All-Payer Claims Database
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=33&art=4A

W. Va. C.S.R. § 114A-01 – All-Payer Claims Database - Data Submission Requirements
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=7428

W. Va. C.S.R. § 114A-02 – All-Payer Claims Database Program's Privacy and Security Rule
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=7429

Principles:

Individual Rights, Security Safeguards

3.18. Breach of Security of Consumer Information Act

W. Va. Code § 46A-2A-101 *et seq.*

Description:

The Breach of Security of Consumer Information Act, W. Va. Code § 46A-2A-101, *et. seq.*, applies to all legal entities, governments, and governmental subdivisions and agencies. Notice or substitute notice is required in the event of a "breach of the security of a system" that one would reasonably believe will result in identity theft or fraud. Breach of the security of a system is defined as "unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information… [and that is] part of a database of personal information." Personal information means the name of an individual linked to unencrypted and unredacted social security number, driver's license or state identification card, or financial account numbers.

Notice, which can be provided by mail, telephone, or electronically, shall include: (1) a description of the categories of information reasonably believed to have been accessed or acquired by the breach; (2) a telephone number or website that can be accessed for the purpose of providing the individual with information about the types of information maintained on the individual or all individuals and whether the entity had information on the specific individual; and (3) information about credit reporting agencies and placing fraud alerts or security freezes. Substitute notice is permitted when the entity can demonstrate cost of notice would exceed fifty thousand dollars, the affected class exceeds one hundred thousand persons, or the entity lacks sufficient contact information. Substitute notice entails two of the following: (i) e-mail notice if the entity has e-mail addresses for the affected class; (ii) conspicuous posting of the notice on the website of the entity; or (iii) notice to major statewide media. An entity can follow its own established notification procedures as long as notice is consistent with the Act. Entities following notification procedures in accord with their primary or functional regulator are deemed to be in compliance. The Act does not apply to Departments subject to Title V of the Gramm-Leach Bliley Act.

The Attorney General has exclusive authority to enforce this Act, including seeking civil penalties, by bringing an action in State Court. However, the statute provides that violations by financial institutions shall be enforceable exclusively by such institution's primary functional regulator. Civil penalties may only be assessed if the defendant has engaged in a course of repeated and willful violations of Article 2A of the WVCCPA.

Implications:

- Departments with existing breach notification procedures should review them for consistency with the Act.
- Departments without breach notification procedures should develop procedures in accord with this Act and applicable West Virginia Executive Branch Privacy Policies.

- Departments should review and consider whether breach notification requirements under HIPAA as amended by HITECH may be applicable on a case by case basis. *See* Sections 1.4.2 and 1.4.3.
- If a breach occurs, Departments should refer to West Virginia Executive Branch Procedure governing unauthorized disclosures: *Response to Unauthorized Disclosures*.

Source:

West Virginia Consumer Credit and Protection Act
W. Va. Code §§ 46A-2A-101 *et seq*. – Breach of Security of Consumer Information
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=46a&art=2A

W. Va. Code § 46A-6-104 – General Consumer Protection, Unlawful acts or practices
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=46a&art=6&section=104#06

W. Va. Code § 46A-6L-101 *et seq.* – Theft of Consumer Identity Protections
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=46a&art=6L

Principles:

Accountability, Notice, Security Safeguards

3.19. Governmental Ethics Act

W. Va. Code § 6B-1-1 *et seq.*
W. Va. C.S.R. § 158-18

Description:

All West Virginia public officials and employees are prohibited from knowingly and improperly disclosing any confidential information acquired in the course of performing official duties. Officials and employees are also prohibited from using such confidential information to further their personal interests or the interests of another. Individuals holding an executive branch position which the Governor has designated by executive order must attend a training course conducted by the Ethics Commission.

Individuals found guilty of violating this section of the Act are guilty of a misdemeanor and can be sentenced to not more than six months in jail or fined no more than one thousand dollars or both.

Implications:

- Supervisors should continuously educate employees about the importance of identifying information that is confidential under State or federal law, rule, or policy and the scope of the proper uses of confidential information.

Source:

W. Va. Code § 6B-2-5 – Ethical standards for elected and appointed officials and public employees
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=06b&art=2&section=5#02

W. Va. Code § 6B-2-5b – Ethics training requirements
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=06b&art=2&section=5B#02

W. Va. C.S.R. § 158-18 – Ethics Training Requirements for Designated Public Officials
https://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=2416

W. Va. Code § 6B-2-10 – Violations and penalties
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=06b&art=2&section=10#02

Principles:

Accountability, Minimum Necessary and Limited Use, Security Safeguards

3.20. Ratification of the National Crime Prevention and Privacy Compact (NCPPC)

W. Va. Code § 15-2-24a

Description:

The NCPPC creates an electronic information sharing system whereby the FBI and participating states can exchange criminal records for non-criminal justice purposes authorized by federal or state law. The Compact, which became effective in 1999, provides reciprocity among the states to share records in a uniform fashion without charging each other for information. West Virginia ratified the Compact and became a participant in 2006. The West Virginia State Police Superintendent is charged with oversight and implementation of the Compact on behalf of the State.

Implications:

- The West Virginia authorized criminal record repository must make all unsealed criminal history records available in response to authorized, non-criminal justice requests.
- Records received from other states must be screened to delete any information not otherwise permitted to be shared under West Virginia law.
- Records produced to other states are governed by the NCPPC and not WV law.

Source:

W. Va. Code § 15-2-24a – National Crime Prevention and Privacy Compact
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=15&art=2&section=24A#02

Principles:

Minimum Necessary and Limited Use

3.21. Chief Technology Officer Duties Relating To Security of Government Information

W. Va. Code § 5A-6-4a
W Va. C.S.R. § 163-01

Description:

The Chief Technology Officer (CTO) and the Office of Technology oversee the statewide coordination of technology for State spending units (not including the Legislature, Judiciary, or State constitutional officers or in most aspects, the Department of Education). The CTO has a duty to ensure the security of State government information, including protecting the data communications infrastructure from unauthorized uses, intrusions, or other security threats. Cleansing, reuse, or retirement of equipment must be accomplished by the Office of Technology. As part of that duty, the CTO is charged with developing policies and procedures to safeguard information systems, data, and communications infrastructures. The CTO must also define the scope and regularity of security audits and which bodies are authorized to conduct security audits. The audits may include on-site visits and reviews of all written security procedures and practices.

Legislation enacted in 2012 clarifies that the CTO is responsible for the cleansing of information technology equipment prior to its retirement or transfer. W. Va. Code § 5A-6-4 (as amended by SB 563, effective June 8, 2012).

Legislation enacted in 2013 adds the Division of Protective Services and the West Virginia Intelligence Fusion Center to the list of agencies exempted from the control of the Chief Technology Officer; it also adds the Treasurer to the list of officers whose responsibilities cannot be encroached upon by the Chief Technology Officer. *See* S. B. 630 (effective April 13, 2013).

Implications:

- Departments need to be prepared to respond to and fully cooperate with authorized security auditors.
- The CTO may direct specific remediation to mitigate findings of insufficient administrative, technical, and physical controls.

Source:

W. Va. Code § 5A-6-4a – Duties of the Chief Technology Officer relating to security of government information
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=05a&art=6&section=4A#06

W. Va. C.S.R. § 163-01 – Procedures for Sanitization, Retirement and Disposition of Information Technology Equipment
https://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=9630

Principles:

3.22. State Board of Education: Student Data Accessibility, Transparency, and Accountability Act

W. Va. Code § 18-2-5h
W. Va. C.S.R. § 126-094

Description:

The Student Data Accessibility, Transparency, and Accountability Act went into effect in June 2014. Under the Act, the Department of Education (DOE) is required to maintain an inventory and index or dictionary of its student data system and develop policies and procedures to ensure that the data inventory complies with FERPA (*See* Section 1.10) and other privacy laws. Access to student data in the statewide system is limited to authorized staff and contractors of the DOE, district employees, students and their parents, and authorized staff of other state agencies pursuant to interagency data-sharing agreements. The DOE must develop a detailed security plan and may not transfer confidential student data unless a specific statutory exception applies. The DOE is also required to notify the governor of new student data proposed for inclusion in the data system, changes to existing data collections, the results of privacy compliance and security audits, and suspected or confirmed breaches.

School districts may not report to the state juvenile delinquency records, criminal records, medical and health records, or student biometric information. Schools may not collect data concerning political affiliation, religious beliefs, sexual orientation, gun ownership, or the results of affective computing.

The state superintendent shall appoint a data governance manager who has the primary responsibility for the privacy policy. Among other things, the state superintendent must ensure the security of technology, ensure compliance with privacy laws, evaluate legislative and regulatory proposals, conduct privacy impact assessments on proposed rules, prepare an annual report to the legislature, ensure that incidents are properly reported, and provide training and education to build a culture of privacy.

Parents must be notified of their right to opt out of their child's data being shared pursuant to data sharing agreements between agencies. They also have the right to inspect and review their child's education record and to request a copy of it.

Recent legislation has strengthened the protection of confidential student data. H.B. 4261, passed on March 12, 2016, amended the Act to expand the prohibition on transferring confidential student data to include "any person or entity, public or private[.]" The bill also creates an exception to the restriction on transferring information related to ACT, SAT, or College Board assessment results, but requires consent if information classified as confidential is required. In addition, the Board of Education has proposed revisions to the current rule governing the collection, maintenance, and disclosure of student data. The revisions would

require a district-level staff member to serve as the local expert on data privacy and governance. The revisions also clarify the need for protocols to terminate data access and the requirements to gain access.

Implications:

- The DOE must ensure that its maintenance of the statewide data system complies with FERPA and other state and federal privacy laws. It must ensure that data is not shared or disclosed to unauthorized individuals, and students and parents must be notified of student privacy rights under federal and state law.
- The DOE must develop procedures and policies to make mandated notifications to the Governor and Legislature.
- School districts must ensure that they do not disclose certain confidential information to the state. They must also notify parents annually of their right to request student information, inform parents of their rights and the process for filing complaints of privacy violations, and ensure that data is only disclosed to authorized individuals.
- Schools must not collect certain individual student data.

Source:

W. Va. Code §18-2-5h – Student Data Accessibility, Transparency, and Accountability Act
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=18&art=2&section=5H#02

West Virginia House Bill 4261
http://www.legis.state.wv.us/Bill_Status/bills_text.cfm?billdoc=HB4261 SUBENR.htm&yr=2016&sesstype=RS&i=4261

W. Va. C.S.R. § 126-094 – Procedures for the Collection, Maintenance and Disclosure of Student Data (Policy 4350)
https://apps.sos.wv.gov/adlaw/csr/rule.aspx?rule=126-094

Principles:

Consent, Security Safeguards, Accountability, Notice

3.23. Confidentiality of Child and Juvenile Records; Sharing Juvenile Records with Other States; West Virginia Child Welfare Act

W. Va. Code §§ 49-1-101 *et seq.*;-2-101 *et seq.*;-3-101 *et seq.*; -4-101 *et seq.*; -5-101 *et seq.*; -6-101 *et seq.*; and -7-101 *et seq.*

Description:

In 2015, the West Virginia State Legislature passed the West Virginia Child Welfare Act through House Bill 2200. The passage of H.B. 2200 resulted in a restructuring of the juvenile justice and welfare law. The legislature "intended to embrace in a revised, consolidated, and codified form and arrangement the laws of the State of West Virginia relating to child welfare at the time of that enactment." While this bill represented a change in the structure of the law and in some places the language of the law, the legislature stated in § 49-1-102 that "[i]t is not the intent of the Legislature, by recodifying the child welfare law of this state during the regular session of the Legislature in the year 2015 to alter the substantive law of this state as it relates to child welfare."

Under this bill, "Confidentiality of Records" is now W. Va. Code § 49-5-101. Under this section, subject to certain statutory exceptions, state agencies may not disclose child or juvenile records or information to anyone, including state and federal agencies. With the exception of adoption records and child abuse or neglect complaints, the child or juvenile records may be disclosed to the child, a parent, and the attorney of the child or parent. They may also be made available with the written consent of the child or upon court order to review the records.

Information relating to child abuse, neglect, fatality, or near fatality, except that which discloses the identity of the person making a complaint, will be made available to various federal, state, and local government entities responsible for protecting children from abuse and neglect. Such information will also be made available to the child fatality review team, child abuse citizen review panels, multidisciplinary investigative and treatment teams, and grand juries, circuit courts and family courts.

Law enforcement juvenile records should be kept separate from adult records and court files. Juvenile records are confidential, except the public has access to the names and identities of juveniles who are tried or convicted in criminal proceedings of violence against another person, possession of a dangerous or deadly weapon, or possession and delivery of a controlled substance. Disclosure to West Virginia public schools cannot occur unless the juvenile is tried and convicted in criminal proceedings of one of those three offenses listed in the previous sentence and attends or will attend the school. S.B. 504, passed March 12, 2016, provides that a recorded or videotaped interview of a minor in a criminal, abuse, or neglect case, and any related documentation, generally is not subject to disclosure.

Juvenile psychological tests and evaluations must never be disclosed except to the school psychologist(s). If the school psychologist, in their professional

judgment, believes disclosure to the principal or other school employees who need to know.

The Division of Juvenile Services (DJS) may provide access and the confidential use of juvenile records to agencies of others states which perform the same function as the DJS, have a reciprocal agreement with the state, and have legal custody of the juvenile in question. The DJS has the authority to enter into reciprocal agreements and may only share information which is relevant to the supervision, care, custody, and treatment of the juvenile.

Willful violation of W. Va. Code §49-5-101 is a misdemeanor, punishable by fines and jail time.

Implications:

State agencies should have policies in place which restrict the disclosure of child or juvenile information or records to those disclosures permitted by the statute.

Source:

W. Va. Code § 49-5-101 – Confidentiality of records; nonrelease of records; exceptions; penalties
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=49&art=5&section=101#05

West Virginia Senate Bill 504
http://www.legis.state.wv.us/Bill_Status/bills_text.cfm?billdoc=SB504 SUB1enr.htm&yr=2016&sesstype=RS&i=504

W. Va. Code § 49-5-103 – Confidentiality of juvenile records; permissible disclosures; penalties; damages
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=49&art=5&section=103#05

W. Va. Code § 49-5-104 – Confidentiality of juvenile records for children who become of age while a ward of the state or who have been transferred to adult criminal jurisdiction; separate and secure location; penalties; damages
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=49&art=5&section=104#05

W. Va. Code § 49-5-106 – Data collection
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=49&art=5&section=106#05

Principles:

Consent, Minimum Necessary and Limited Use, Security Safeguards

3.24. Monitoring Inmates Telephone Calls and Mail

W. Va. Code §§ 25-1-17 and -18

Description:

This legislation authorizes the Commissioner of Corrections to monitor, intercept, open, record, and copy telephone calls and mail to inmates of state correctional institutions. Inmates must be notified in writing of these potential actions. The contents of these communications may be disclosed to law enforcement agencies pursuant to an order of a court or administrative tribunal when necessary for the following reasons: to investigate, prosecute, or prevent a crime; to safeguard the orderly operation of the correctional institution; or to protect persons from harm or the threat of physical harm. Attorney-client communications are exempt from these requirements.

S.B. 262, passed on March 12, 2016, amends §§ 25-1-17 and -18. Law enforcement officials no longer need to obtain a court order prior to receiving communications for investigative purposes. If the monitored communication leads to an indictment, the inmate's attorney is entitled to the conversation. Finally, the bill clarifies that the provisions on monitoring apply only to persons in the physical custody of the Commission of Corrections.

Implications:

- The Department of Corrections must have policies in place to comply with these statutes.
- The Department of Corrections must give clear guidance as to when a court order shall be sought before notifying law enforcement officials.
- The Department of Corrections must retain recordings and copies of these communications for at least three years and then destroy them in accordance with its record retention policy.

Source:

W. Va. Code § 25-1-17 – Monitoring of inmate telephone calls; procedures and restrictions; calls to or from attorneys excepted
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=25&art=1&section=17#01

W. Va. Code § 25-1-18 – Monitoring inmate mail; procedures and restrictions; identifying mail from a state correctional institution; mail to or from attorneys excepted
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=25&art=1&section=18#01

West Virginia Senate Bill 262
http://www.legis.state.wv.us/Bill_Status/bills_text.cfm?billdoc=SB262 SUB1 enr.htm&yr=2016&sesstype=RS&i=262

Principles:
Accountability, Notice

3.25. Drug Testing for Public Improvements

W. Va. Code §§ 21-1D-2, -7a, -7b, -8

Description:

The West Virginia Alcohol and Drug-Free Workplace Act, W. Va. Code § 21-1D-1 *et. seq.* requires that contractors constructing a public improvement maintain a drug free workplace policy. Not less than once per year, or upon completion of the project, every such contractor shall provide a certified report to the public authority which let the contract to show the following: what educational efforts were undertaken with employees; what federally certified laboratory conducted the testing; and the number of positive and negative drug tests conducted at the time of pre-employment, upon reasonable suspicion, post-accident, and at random. Failure to comply with this law is a misdemeanor.

Implications:

- Public authorities must develop compliance efforts to assess the contractor's implementation of the drug-free workplace policy.
- Contractual documents shall be amended to include the requirement for the maintenance of a drug-free workplace policy by the contractor, subcontractors doing business with the contractor, municipalities, and municipal political subdivisions.

Source:

West Virginia Alcohol And Drug-Free Workplace Act
W. Va. Code §21-1D-2 – Definitions
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=21&art=1D&section=2#01D

W. Va. Code § §21-1D-7a – Confidentiality; test results not to be used in criminal and administrative proceedings
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=21&art=1D&section=7A#01D

W. Va. Code § 21-1D-7b – Contractor to provide certified drug-free workplace report
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=21&art=1D&section=7B#01D

W. Va. Code § 21-1D-8 – Penalties for violation of this article
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=21&art=1D&section=8#01D

Principles:

Accountability, Notice, Security Safeguards

3.26. Verifying Legal Employment Status of Workers

W. Va. Code § 21-1B-1 *et seq.*
W. Va C.S.R. § 42-31

Description:

This law places the responsibility on employers to verify the legal employment status of all persons who come into their employ, maintain appropriate records of proof of work authorization, and report their employment to the appropriate governmental agencies. "Employer" is defined as any individual, person, corporation, department, board, bureau, agency, commission, division, office, company firm, partnership, council or committee of the state government, public authority, or political subdivision of the state, or other business entity which employs individuals. The Labor Commissioner is authorized to access information maintained by any other state agency for the limited purpose of confirming the validity of a worker's legal status or authorization to work. There is a penalty for an employer's failure to maintain certain records. The Commissioner is authorized to issue notices to employers to produce records or documents to verify the legal status of an employee and to terminate undocumented employees.

On July 1, 2015, updated regulations took effect. These regulations amend the type and number of accepted documents employers must use to verify legal status, explain how the Commissioner may issue a citation to employers, and clarify what type of information the Commissioner may obtain from an employee.

Implications:

- Departments must have policies and procedures in place to verify the legal status of employees and prospective applicants for employment.
- Departments should give Notice to prospective applicants that a verification of legal status for employment will be conducted; that notice should include what information may be accessed or disclosed as a result of such verification.
- Departments must review the regulations to ensure compliance with documentation requirements to verify the legal status of employees.

Source:

W. Va. Code § 21-1B-2 – Definitions
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=21&art=1B&section=2#01B

W. Va. Code § 21-1B-3 – Unauthorized workers; employment prohibited
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=21&art=1B&section=3#01B

W. Va. Code § 21-1B-4 – Record-keeping requirements; employer compliance

http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=21&art=1B&section=4#01B

W. Va. Code § 21-1B-5 – Penalties
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=21&art=1B&section=5#01B

W. Va. Code § 21-1B-7 – Suspension or revocation of license
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=21&art=1B&section=7#01B

W. Va. C.S.R. § 42-31. – Verifying the Legal Employment Status of Workers
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=9496

Principles:
Accountability, Notice

3.27. Address Confidentiality Program

W. Va. Code §§ 48-28A-101 to -110
W. Va. C.S.R. § 153-37

Description:

This law established an Address Confidentiality Program in the Secretary of State's Office pursuant to which persons attempting to escape from actual or threatened domestic violence, sexual assault, or stalking may establish a designated address in order to prevent their assailants or probable assailants from finding them. A person may apply to the Secretary of State to participate in this program. Upon approval of the application, the Secretary of State assigns the applicant a designated address, which state and local agencies and courts of this State are required to accept for the purpose of creating a new public record. The designated address is used by the Division of Motor Vehicles on the applicant's driver's license or identification card, and the designated address or a post office box may be used by the applicant for voter's registration purposes. Procedures are provided under which the applicant's residential or mailing address is available to law enforcement officers and to the head of a state agency or designee under prescribed circumstances. Disclosure may also be made pursuant to a court order. The program participant's application and supporting materials are not public records. Willful unauthorized disclosure is a misdemeanor punishable upon conviction by a fine or imprisonment in a regional jail. Participation in this program is renewable every four years unless participation is cancelled.

Implications:

- The Secretary of State was required to propose legislative rules for promulgation; the rules facilitating the administration of the program were adopted and amended in 2013.
- Courts and agencies of this State that receive the participant's residential or mailing address from the Secretary of State are required to keep that information confidential.

Source:

W. Va. Code §§ 48-28A-101 to -110 – Address Confidentiality Program
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=48&art=28A

W. Va. C.S.R. § 153-37 – Administration of Address Confidentiality Program
http://apps.sos.wv.gov/adlaw/csr/ruleview.aspx?document=8652

Principle:

Security safeguards

3.28. Security of Capital Complex, Other State Facilities, and Sensitive or Critical Information

W. Va. Code § 15-2D-3

Description:

Any service provider whose employees are regularly employed on the grounds or in the buildings of the Capitol Complex or who have access to sensitive or critical information may be required by the Director of the Division of Protective Services, Department of Military Affairs and Public Safety, to submit to a fingerprint-based state and federal background inquiry through the state repository. The Director may also require a new employee who is employed to provide services on the grounds or in the building of the Capitol Complex to submit to an employment eligibility check through E-verify. W. Va. Code § 15-2D-3(e).

After the contract for these services has been approved, but before any such employees are permitted to be on the grounds or in the buildings of the Capitol Complex or have access to sensitive or critical information, the service provider must submit a list of all persons who will be physically present and working at the Capitol Complex for purposes of verifying compliance with W. Va. Code § 15-2D-3.

All current service providers must ensure that all of their employees who are providing services on the grounds or in the buildings of the Capitol Complex or who have access to sensitive or critical information submit to a fingerprint-based state and federal background inquiry through the state repository.

Any contract entered into, amended, or renewed by an agency or entity of state government with a service provider must now contain a provision reserving the right to prohibit specific employees thereof from accessing sensitive or critical information or to be present at the Capitol Complex based upon results addressed from a criminal background check.

For purposes of section 3, the term “service provider” means any person or company that provides employees to a state agency or entity of state government to work on the grounds or in the buildings that make up the Capitol Complex or who have access to sensitive or critical information.

In accordance with the provisions of Public Law 92-544 the criminal background check information is to be released to the Director of the Division of Protective Services.

Implications:

All agencies with offices at the Capital Complex should ensure that its outside service providers who work at the Capital Complex, will work at the Capital Complex, or will have access to sensitive or critical information comply with the new requirements of W. Va. Code § 15-2D-3.

Source:

W. Va. Code § 15-2D-3 – Duties and powers of the director and officers
http://www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=15&art=2D&section=3#02D

Principle:

Security Safeguards

4.0. Agency Agreements with Privacy or Security Provisions

Description:

State Government contracts with vendors for products and services may require the vendor to receive or create PII or other confidential information; if so, the contract will include a requirement to notify the State agency of a breach of security or privacy. Where a vendor receives or creates PII or other confidential information from or on behalf of the State, the vendor shall receive notice of the State's policy regarding the security and privacy of the information and agree to certain terms and conditions. Further, where the contracting Department is either a Covered Entity or Business Associate and PHI is or may be disclosed to the vendor, the Department shall ensure the vendor agrees to and executes the State Government Business Associate Addendum. *See* Section 1.4.1 for a discussion of recent changes allowing disclosure for firearm background checks.

Implications:

- Departments shall ensure that the Purchasing Division's General Terms & Conditions are included within all contracts. The General Terms & Conditions are located at http://www.state.wv.us/admin/purchase/TCP.pdf. Use of the Purchasing Division's forms will facilitate compliance.
- Any HIPAA Covered Entities or Business Associate departments shall ensure that the West Virginia State Government HIPAA Business Associate Addendum is included in all contracts. Agencies and vendors should ensure they are using the revised Business Associate Addendum in their contracts. All contracts with Business Associates must comply with the Final Rule.
- Departments which must be HIPAA compliant should assure that their Business Associates are in compliance with this Business Associate Addendum.
- Those acting as Business Associates will review and revise their policies, procedures, and practices in light of the HITECH Act amendments to HIPAA, all applicable federal HIPAA regulations, and any subsequently issued applicable regulations, including but not limited to the Final Rule.
- Departments will monitor the law and attain compliance within the specified time periods as may be applicable.

Source:

WV State Government HIPAA Business Associate Addendum
http://www.state.wv.us/admin/purchase/vrc/WvBaaAgEffectiveJun2013.pdf

Notice to Vendors Regarding Compliance with Final Rule
http://www.state.wv.us/admin/purchase/privacy/baa_notice.pdf

HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act

45 C.F.R. Part 160 – General Administrative Requirements
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=d3e10d0edbd4821f4608f5d620fc85ba&rgn=div5&view=text&node=45:1.0.1.3.75&idno=45

45 C.F.R. Part 164 – Security And Privacy
http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=d3e10d0edbd4821f4608f5d620fc85ba&rgn=div5&view=text&node=45:1.0.1.3.78&idno=45

Modifications to the HIPAA Rules – Final Rule
http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

Principles:
Accountability, Security Safeguards, Notice, Individual Rights

4.1. Vendor Agreement Clauses

Description:

The HIPAA Business Associate Addendum is a part of State agency contracts where the vendor is a “Business Associate” as that term is broadly defined in 45 C.F.R. 160.103. In general, any vendor that will directly or indirectly have access to PHI is a Business Associate.

This Addendum, among other things:

1. Prohibits the Business Associate from using or disclosing PHI in a manner in violation of existing law and specifically in violation of laws relating to confidentiality of PHI, including but not limited to, the Privacy and Security Rules. HIPAA Business Associate Addendum Section 3 (obligations of associate), Subsection (d) (compliance with law).

2. Obligates the Business Associate to mitigate, to the extent practicable, any harmful effect that is known to the Associate of a use or disclosure of PHI by the Business Associate in violation of the requirements of the Business Associate Addendum, and to report its mitigation activity back to the applicable State agency. HIPAA Business Associate Addendum Section 3 (obligations of associate), Subsection e (mitigation).

3. Obligates the Business Associate to take all steps necessary to ensure the continuous security of all PHI and data systems containing PHI. HIPAA Business Associate Addendum Section 3 (obligations of associate), Subsection k (security).

4. Obligates the Business Associate to notify the applicable State agency and, unless otherwise directed by the agency in writing, the Office of Technology immediately by e-mail or web form upon the discovery of breach of security of PHI, where the use or disclosure is not provided for in the Business Addendum or was acquired by an unauthorized person, or within 24 hours by e-mail or web form of any suspected incident, unauthorized use or disclosure in violation of Business Addendum or potential loss of confidential data affecting the Addendum. HIPAA Business Associate Addendum Section 3 (obligations of associate), Subsection l (notification of breach).

5. Additionally, the Business Associate is required to immediately investigate the Security incident, breach, or unauthorized use or disclosure of PHI or confidential data and notify the applicable State agency contract manager in writing, within 72 hours, regarding (a) Date of discovery; (b) What data elements were involved and the extent of the data involved in the breach; (c) A description of the unauthorized person known or reasonably believed to have improperly used or disclosed PHI or confidential data; (d) A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized;

(e) A description of the probable causes of the improper use or disclosure; and (f) Whether any federal or state laws requiring individual notifications of breaches are triggered. *Ibid*.

Because the Attorney General approves purchasing contracts as to form, the HIPAA Business Associate Addendum is most likely incorporated into all vendor contracts with a government agency, such as BMS, the Office of Insurance Commissioner, PEIA, or any other agency that has HIPAA information, when the vendor will directly or indirectly have access to that HIPAA information. *See* the first paragraph of the HIPAA Business Associate Addendum.

Additionally, the State Purchasing Division's Instructions to Vendors Submitting Bids requires vendors to agree to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws. *See* paragraph 45 (indemnification), Purchasing Division's General Terms and Conditions, Instructions to Vendors Submitting Bids, at
http://www.state.wv.us/admin/purchase/TCP.pdf

5.0. West Virginia Case Law

A. State Freedom of Information Act Cases

1. *In re Charleston Gazette FOIA Request*, 222 W. Va. 771, 671 S.E.2d 776 (2008).

In *Gazette*, the newspaper had submitted a FOIA request to the City of Charleston requesting copies of weekly payroll time sheets and activity logs for certain named police officers employed by the Charleston Police Department (CPD) following public allegations that some police officers were "double-dipping." It was alleged that while these police officers were on duty for the City, they were also employed at the very same time by private entities as security guards, and that they were collecting two pay checks at the same time -- one from the City and one from the private employer.

The City denied the FOIA request and provided four reasons for the denial. First, the City stated that some of the documents sought by the Gazette directly pertained to an ongoing criminal investigation being undertaken by the CPD. Second, the City stated that Kanawha County Circuit Judges had issued protective orders in proceedings separate from the Gazette's request, sealing the records of six of the 28 officers who were the subject of the Gazette's document request. Third, the City indicated that it was uncertain about releasing the documents in question because Judge Walker ruled, when similar information was sought by a defendant for use in his criminal case, that the type of information requested by that defendant, some of which would have to be obtained from personnel files, together with the proffer of the CPD about that information, would trigger the protections afforded under *Manns v. City of Charleston Police Department*, 209 W. Va. 620, 550 S.E.2d 598 (2001), and *Maclay v. Jones*, 208 W. Va. 569, 542 S.E.2d 83 (2001). Fourth, the City explained that it had received a letter from the Fraternal Order of Police, Capitol City Lodge 74, on behalf of some or all of the officers whose records were requested by the Gazette, requesting that the City not produce these records absent a court order. The Gazette replied to the City's response by disputing the City's reasons for non-disclosure and asking the City to reconsider its refusal to provide the requested documents. The City then filed a complaint for declaratory judgment in the Circuit Court of Kanawha County. However, before the Gazette filed a response, the circuit court dismissed the City's complaint, *sua sponte*, reasoning that an order in the case would not be of practical assistance in settling the controversy as to the documents not under seal and that as to the documents under seal, they would remain under seal and the underlying controversy in the matter would persist. The City then filed a motion to alter or amend judgment. The circuit court entered an amended order and again dismissed the complaint. The City appealed the circuit court's final order to the Supreme Court of Appeals.

Ruling:

The West Virginia Supreme Court of Appeals concluded that the Gazette was entitled to inspect and copy the payroll records and that the Circuit Court of Kanawha County erred with regard to its *sua sponte* dismissal of the City's declaratory judgment action. The Court again held that the disclosure provisions of this State's FOIA are to be liberally construed, and that exemptions to the Act are to be strictly construed, citing Syl. Pt. 4, *Hechler v. Casey*, 175 W. Va. 434, 333 S.E.2d 799 (1985). Additionally, the Court again held that in deciding whether the public disclosure of information of a personal nature under W. Va. Code § 29B-1-4(a)(2) would constitute an unreasonable invasion of privacy, the Court will look to five factors: (1) whether disclosure would result in a substantial invasion of privacy and, if so, how serious; (2) the extent or value of the public interest, and the purpose or object of the individuals seeking disclosure; (3) whether the information is available from other sources; (4) whether the information was given with an expectation of confidentiality; and (5) whether it is possible to mould relief so as to limit the invasion of individual privacy, citing Syl. Pt. 2, *Child Protection Group v. Cline*, 177 W. Va. 29, 350 S.E.2d 541 (1986), and Syl. Pt. 4, *Manns v. City of Charleston Police Dept*., 209 W. Va. 620, 550 S.E.2d 598 (2001). Lastly, the Court held that exemption 29B-1-4(a)(4) did not apply because the requested records were generated as part of an administrative function and were not generated in the detection and investigation of a crime. The fact that some of the administrative records were being used in an investigation did not prevent them from being disclosed to the Gazette. The Court also found that while some of the records were under circuit court ordered protective seal, an agreement of the parties in those cases to seal certain records did not operate to protect the records from discovery under FOIA.

Implications:

- When agencies respond to a State FOIA requests, they should keep in mind that the general policy of the State FOIA is to allow as many public records as possible to be available to the public. Therefore, the State FOIA is liberally construed and exemptions from disclosure are narrowly construed.

- State FOIA Exemptions:
  - While W. Va. Code § 29B-1-4(a)(2) exempts from disclosure information of a personal nature such as that kept in a personal, medical or similar file if the public disclosure would constitute an unreasonable invasion of privacy, this is not a "blanket" or *per se* exemption. The information must be disclosed when the public interest, by clear and convincing evidence, requires disclosure in the particular instance because the primary purpose of this exemption is to protect individuals from the injury and embarrassment that can result from the unnecessary disclosure of personal information. Syl.Pt. 6, *Hechler v. Casey*, 175 W. Va. 434, 333 S.E.2d 799 (1985). Consequently, application of exemption (a)(2) requires courts, and therefore agencies in the first instance, to balance or weigh the individual's right of privacy against the public's right to know. See

Syl. Pt. 1, *Child Protection Group v. Cline, supra*. Additionally, the *Gazette* case should not be construed as delineating the precise scope of the right to privacy afforded by exemption 29B-1-4(a)(2). The *Gazette* Court simply believed that the requested records did not include the kind of private facts that the Legislature intended to exempt from mandatory disclosure.

- While the W. Va. Code § 29B-1-4(a)(4) exemption from disclosure includes records of law-enforcement agencies that deal with the detection and investigation of crime and the internal records and notations of such law-enforcement agencies which are maintained for internal use in matters relating to law enforcement, this exemption is likewise not a "blank" or *per se* exemption. *Compare Manns v. City of Charleston Police Dept*., 209 W. Va. 620, 550 S.E.2d 598 (2001), with *In re Charleston Gazette FOIA Request, supra*. The distinguishing fact, as between *Manns* and *Gazette*, is that in *Manns* the request was for confidential information provided by third-party public citizens, while in *Gazette* the request was for information provided by public employees, involved ministerial payroll information, and was not information provided as part of an internal investigation document. *See* Syl. Pt. 11, *Hechler v. Casey*, 175 W. Va. 434, 333 S.E.2d 799 (1985) (the investigatory records exemption in FOIA does not include "information generated pursuant to routine administration or oversight, but is limited to information compiled as part of an inquiry into specific suspected violations of the law").

  - While Justice Benjamin concurred in the decision in *Gazette*, he filed a concurring opinion to underscore the importance of the statutory exemption from disclosure of records which deal with the detection and investigation of crimes. W. Va. Code § 29B-1-4(a)(4). Justice Benjamin believed that while this exemption did not apply in the *Gazette* case, in other situations the release of payroll records could carry with it the release of related information, such as the location of undercover work by a law enforcement officer, which could otherwise compromise a criminal investigation and that exemption 4(a)(4) should apply to those payroll records.

- To some degree, expectations of privacy of a public employee should be different from that of a private sector employee. The *Gazette* opinion cites and discussed the opinion in *Perkins v. Freedom of Info. Comm'n*, 228 Conn. 158, 635 A.2d 783 (1993). In that case, the Connecticut Supreme Court held that a FOIA request for the numerical data dealing with a public employee's sick leave records did not constitute a *per se* invasion of personal privacy writing "when a person accepts public employment, he or she becomes a servant of and accountable to the public. As a result, that person's reasonable expectation of privacy is diminished, especially in

regard to the dates and times required to perform public duties." The Connecticut Court further stated that "The public has a right to know not only who their public employees are, but also when their public employees are and are not performing their duties." 228 Conn. at 177, 635 A.2d at 792.

2. *The Associated Press v. Canterbury*, 224 W. Va., 708, 688 S.E.2d 317 (2009).

The issue in Associated Press was whether thirteen e-mail communications sent by Justice Maynard to Mr. Don Blankenship were subject to disclosure as public records under the State Freedom of Information Act (FOIA). In addition to this substantive issue, this case presents an important procedural issue under FOIA concerning the circuit courts' in camera review of the thirteen e-mails

Ruling:

The West Virginia Supreme Court of Appeals held that a personal e-mail communication sent from a government e-mail account by a public official or public employee, which does not relate to the conduct of the public's business, is not a public record subject to disclosure under FOIA. The Court determined that e-mail is a "writing" and therefore a public record for purposes of FOIA analysis. In response to a public official's refusal to produce FOIA-requested records, a trial court may, in its discretion and on its own motion, order the production of records withheld by a public official. The trial court then reviews the records to determine whether any of the records are subject to disclosure under FOIA. This analysis is restricted to the content of the e-mail and is not driven by the context, that is, how and where the e-mail was created.

Implications:

- The Court's holding establishes that public employees can expect some degree of privacy from public scrutiny when sending e-mail messages of a personal nature from work accounts. The analysis hinges on the Court's interpretation that state law defines a public record by its content not its context nor where it is created and stored. For purposes of public disclosure, it is not enough that communication occurs on a government issued phone, computer, or device — it also has to be a communication about government business.

- However, public employees' non-work-related e-mails and text messages transmitted on government provided equipment may be subject to their employer's review. The United States Supreme Court determined in *Ontario v. Quon* (*see* Federal Case Law, Section 2.0) that a governmental employer had a legitimate interest in reviewing the text messages that an employee sent during working hours from his employer-provided pager and that the employer's review of such messages did not violate the employee's Fourth Amendment rights. The Court noted that if a search is conducted for "noninvestigatory, work-related purposes" or for "investigations of work-

related misconduct," it may be reasonable if it is "justified at its inception" and if the measures used are "reasonably related to the objectives of the search" and are not "excessively intrusive."

- In contrast to *Canterbury, Quon* holds that while assuming employees may have an expectation of privacy in their communications sent on government-owned devices, the government employer may review the messages if the employee has knowledge of the organization's policy [of its right to review all workplace communications], the review is motivated by a legitimate work-related purpose, and the review is not excessive in scope. A government employer's review of its employees' text messages for a legitimate, work-related purpose is not the same as a FOIA request to access an employee's personal communications that are not related to the public's business.

3. *Shepherdstown Observer, Inc. v. Maghan*, 226 W. Va. 353, 700 S.E.2d 805 (2010).

In *Maghan*, the newspaper had filed a state Freedom of Information Act request with the county clerk seeking all certification documents for the then-proposed zoning referendum, including the petition and the signatures thereon. On the theory that the petition and signatures were not a public record as defined in the Act, the county clerk denied the request. The newspaper filed a civil action to compel the disclosure. The circuit court agreed with the county clerk, finding that the petition and signatures was not a public record because the document had not been prepared by the county commission nor had it been prepared at the request of the county commission.

On appeal to the Supreme Court of Appeals, two categories of issues were presented to the Court. The first category related to the interpretation and application of the state Freedom of Information Act, W. Va. Code § 29B-1-1, *et seq*. The second category related to the constitutional issues of whether the signatures on a zoning referendum petition are tantamount to a secret ballot, whether the release of those signatures would have a "chilling effect" on the freedom to petition the government, and whether a valid public purpose exists for the disclosure of referendum petitions under the W. Va. Freedom of Information Act.

Ruling:
The Supreme Court of Appeals reversed the decision of the circuit court and held that under the state Freedom of Information Act, a "public record" includes any writing in the possession of a public body that relates to the conduct of the public's business which is not specifically exempt from disclosure by W. Va. Code § 29B-1-4, even though the writing was not prepared by, on behalf of, or at the request of the public body. Accordingly, the Court held that a referendum petition filed with a public body is a public record required to be disclosed under the Act.

Implications:

In responding to a state Freedom of Information Act request, agencies may no longer claim that a document in their possession is not subject to disclosure just because the document was prepared by a third party. Documents relating to the conduct of the public's business need to be disclosed unless one of the exemptions in W. Va. Code § 29B-1-4 applies to the document.

4. *Charleston Gazette v. Smithers*, 232 W. Va. 449, 752 S.E.2d 603 (2013).

In *Charleston Gazette v. Smithers*, the court was faced with the question of whether the state police must disclose information gathered in relation to allegations of misconduct and incidents of use of force. The Gazette filed suit in 2010 following a State Police denial of certain FOIA requests made by reporter Gary Harki. The exact details of the requested documents were not on record for the court to review, but it was aware that the language of the requests was taken directly from certain legislative rules and code sections which describe the State Police review process. Mr. Harki requested data provided to the Internal Review Board, a copy of the central log of complaints, and reports of the Internal Review Board with those employees identified by the Early Identification System redacted. The circuit court dismissed the complaint with prejudice, concluding that all of the requested documents were exempt from disclosure as either an unreasonable invasion of privacy, internal memorandum of a public body, or documents dealing with the detection and investigation of crime.

Ruling:

Justice Workman, writing for the court, began by noting that FOIA is to be "liberally construed" and that the burden is on the party seeking exemption to prove the "applicability of such exemption to the material requested." The first exemption relied upon by the State Police was the invasion of privacy exemption in W. Va. Code §29B-a-4(a)(2); this exemption deals with "information of a personal nature such as that kept in a personal, medical or similar file" which is exempt unless the public interest outweighs the private interest. The Gazette asserted that many other courts have concluded that police officers do not have a privacy interest in complaint and review records, but the court found this assertion unconvincing because the Gazette neglected to distinguish "between policy-based decisions and those predicated upon the language of a specific state statute," which would reveal that there is no bright line rule. Because there was a lack of meaningful analysis, the court chose not to apply its holding in *Manns v. City of Charleston Police Department*, 550 S.E.2d 598, 600-04 (W. Va. 2001), where a request for "the names of every officer against whom a complaint has been made" or "against whom a civil or criminal complaint has been filed" and "the outcome of said complaints or investigations" was denied as being an invasion of privacy that would quell "continued reports of possible misconduct."

Instead, the court chose to apply the following factors that it adopted in *Child Protection Group v. Cline*, 350 S.E.2d 541 (W. Va. 1986), to analyze whether the invasion of privacy exemption applied: whether disclosure would result in a substantial invasion of privacy and, if so, how serious; the extent or value of the public interest and the purpose or object of the individuals seeking disclosure; whether the information is available from other sources; whether the information was given with an expectation of confidentiality; and whether it is possible to mold relief so as to limit the invasion of individual privacy. The court concluded that disclosure related to on-the-job activities of a police officer are not unreasonable and that the Gazette had a legitimate interest in publishing the sought after information. The parties both stipulated that the information could not be obtained elsewhere. Despite the fact that the legislative rule dictated that the information be confidential, the court concluded that in order to harmonize the rule with FOIA, it should be used only as one factor in the analysis. Lastly, the court concluded that the best way to both allow disclosure and limit invasion of privacy was to mandate disclosure only after an investigation has taken place and a determination had been made. Due to the lack of clarity concerning requested disclosures, the court concluded that the above factors would have to be applied to a more factually developed record on remand.

In regard to the law enforcement exemption, the court concluded the State Police had not shown with enough specificity the information which it sought to keep from disclosure. The State Police expressed concern that certain complaints would contain information related to ongoing investigations, but they did not fulfill their burden to show the exemption applied to specific complaints. Likewise, in arguing that some of the information would be subject to exemption as an internal memorandum, the State Police failed to specifically show what records should be exempted. Because internal memorandums are only exempted if they consist of "advice, opinions, and recommendations which reflect a public body's deliberative, decision-making process," the State Police had a burden to show this exemption applied, and they failed to do so. Therefore, because the invasion of privacy, law enforcement, and internal memorandum exemptions did not apply based on the current record, the court reversed and remanded the case with instruction for the circuit court to review the disputed documents.

Implications:

- The court will not require a government entity to disclose the details of ongoing disciplinary investigations. However, agencies should be prepared to disclose the results of internal investigations after a determination has been made. According to the court, this limits the invasion of privacy for individuals who are under investigation and also allows for the public to be made aware of the results of investigations after the fact, whether positive or negative.
- As a practical matter, it is important for agencies to be specific when denying FOIA requests as statutory exemptions. The court requires not only that statutory reasons be given but that those reasons, along with the

harm that disclosure would cause, be linked specifically to documents which the agency determines fall under the exemption. The exemptions are not blanket exceptions to the favoring of disclosure and apply only to specific situations which the legislature and court has outlined. Therefore, without compromising the material, it is important to specifically designate documents and the reason that they should not be disclosed.

5. *King v. Nease*, 233 W. Va. 252, 757 S.E.2d 782 (2014).

The case of *King v. Nease* involved an ordinance in the City of Nitro which imposed fees to cover the cost of an employee's time and photocopying expenses in producing certain paper records in response to a FOIA request. The City of Nitro indicated to the plaintiffs that it would only produce a number of the requested documents if they agreed to cover a search fee. The issue before the court was whether the legislature had meant to include such search fees when it said in W. Va. Code §29B-1-3(5) that "the public body may establish fees reasonably calculated to reimburse it for its actual cost in making reproductions of such records." The circuit court initially concluded that the phrase "actual cost in making reproductions" was meant only to apply to the actual cost of making copies, not an employee's time.

Ruling:

The Supreme Court, however, reasoned that the circuit court had erroneously limited its analysis by neglecting to discuss the term "fees" which is defined as a "charge for labor or services." Based on this language and the fact that the legislature had formally approved agency-specific search fees in the past, the court concluded that "there can be no dispute that search fees may be included as part of a FOIA request."

Justice Benjamin filed a dissenting opinion in which he criticized the majority for injecting ambiguity where he thought the statute was only susceptible to one reasonable construction. He argued that the majority considered the word "fees" in isolation and neglected to note that the "fees" are to cover the "actual cost in making reproductions." Although the majority took great care to explain that it was only asked to make a holding based on statutory construction, not the public policy of FOIA, Justice Benjamin maintained that "the amount that a public body may charge for the production of records directly affects the disclosure of records." He viewed the charging of a retrieval or search fee as a direct attack on the transparency and legitimacy of government that would have "a chilling effect on citizens who desire access to government records."

Implications:

The results of the holding in Nease are fairly straight forward. Public bodies have always been able to charge a fee for the copies of documents requested by members of the public; however, after Nease, public bodies may charge a search or retrieval fee to cover the cost of paying an employee whose time is part of the "actual cost in making reproduction." Although the present case dealt with a city

ordinance applying search fees for extensive production of files not in digital format, it seems that any amount of employee time spent on a FOIA request could be charged as a fee if properly recorded. Such a policy could help to reduce costs and may limit frivolous requests.

6. *Hurlbert v. Matkovich*, 233 W. Va. 583, 760 S.E.2d 152 (2014)

Robert Hurlbert, a California resident, ran a business that sought to ferret out mortgage fraud by examining appraisal data. He requested assessment and Computer-Assisted Mass Appraisal ("CAMA") files from the Tax Commissioner. CAMA files are generated by county assessors who input data into a statewide Integrated Assessment System maintained and administered by the Tax Commissioner. While the assessment files are a compilation of information already contained in publicly-available land books, CAMA files contain more detailed information, including sensitive or personal information, business secrets, and information which might present homeland security issues.

The Tax Commissioner released the assessment files but denied the request for the CAMA files, arguing that the county custodians were the custodians of those records. Hurlbert then sought declaratory judgment and injunctive relief in Kanawha County Circuit Court. After the Kanawha County Assessor intervened, the circuit court granted summary judgment to the Tax Commissioner and the Assessor, concluding that the CAMA files fell under the property tax return exemption (W. Va. Code § 11-1A-23(a)) and trade secrets exemption (W. Va. Code § 29B-a-4(a)(1)). The court also held that the CAMA files met the first prong of the *Cline* test, i.e., a substantial invasion of privacy.

Ruling:

On appeal, the Supreme Court of Appeals of West Virginia reversed and remanded in a *per curiam* opinion. The court considered three issues: (1) Whether the Tax Commissioner is the "custodian" of the records; (2) Whether the CAMA files are categorically exempt from disclosure; and (3) Whether the circuit court erred by not requiring a *Vaughn* index.

As to the first issue, the court held that the Commissioner was the "custodian" of the CAMA files. The court, in line with its own precedents giving "custodian" a liberal construction, reasoned that the documents were in the "possession" of the Tax Commissioner in addition to being prepared "on behalf of" and "at the request of" the Tax Commissioner. 233 W. Va. at 589-90, 760 S.E.2d at 157-58. The court noted that "exercis[ing] control" over the documents would be sufficient to make a public body the "custodian" of a record. *Id.* at 590, 760 S.E.2d at 158.

As to the second issue, the court held that the CAMA data was not categorically exempt from disclosure. The court used canons of statutory construction to conclude that the Legislature had not intended to make all of the CAMA data confidential since "return information" referred to information provided on the tax

return document and specific exemptions had been made for security systems and other sensitive information. The court also clarified that neither West Virginia citizenship nor a non-commercial purpose were prerequisites to making an FOIA request.

Although the circuit court had correctly exempted some portions of the data, the court held that it had erred by finding a blanket exemption when only some of the data fell within the narrowly-defined exemptions. The court found that the CAMA data did not constitute *per* se "personal information." For example, information related to the construction and general characteristics of the property did not constitute "personal information."

As to the third issue, the court held that the circuit court should have required the Commissioner and the Assessor to submit a *Vaughn* index. A *Vaughn* index (named for *Vaughn v. Rose*, 484 F.2d 820 (D.C. Cir. 1973) provides a detailed justification based on the statutorily designated exemptions for why each document is exempt from disclosure. The index must be provided when segregation or redaction would impose an unreasonably high burden or expense. The court rejected the Tax Commissioner's conclusory statement and criticized the failure to produce an estimate on the cost of redacting the information. The court heavily criticized "sweep[ing] an entire database of information under a general allegation of exemption[.]" 233 W. Va. at 596, 760 S.E.2d at 165.

In dissent, Justice Ketchum argued that details about the interior of the home constituted a substantial invasion of privacy. Justice Ketchum also considered the business purpose for the request to be antithetical to a public interest requiring disclosure. Justice Loughry, writing in concurrence, invited the Legislature to reconsider whether FOIA requests should be limited to state citizens. He reasoned that the FOIA served the purpose of government transparency and accountability, a concern uniquely tied to the citizens of the relevant government.

Implications:

Departments should evaluate which records they may be the "custodian" of and develop a procedure for creating a *Vaughn* index when redacting exempt information is not feasible. Additionally, departments should recognize that citizenship, commercial purpose, and the exemption of some data are not categorical exemptions from disclosure.

7. *Highland Mining Co. v. West Virginia University School of Medicine*, 235 W. Va. 370, 774 S.E.2d 36 (2015).

During the course of several years of discussion and litigation, Highland Mining Co. brought suit against West Virginia University ("WVU") seeking disclosure of public records under the West Virginia FOIA. WVU professor Michael Hendryx had published articles suggesting surface coal mining play a role in health issues for area residents. Highland Mining sought documents that supported those findings,

arguing they were necessary to support its arguments. WVU released several hundred documents, but refused to release some of the documents Highland requested, claiming they were exempt. The lower court agreed, and dismissed Highland's complaint.

The Supreme Court of Appeals of West Virginia found that: "(1) WVU may invoke the FOIA's "internal memoranda" exemption set forth in West Virginia Code § 29B-1-4(a)(8) to withhold documents that reflect Professor Hendryx's deliberative process; (2) WVU may not claim an "academic freedom" privilege to avoid the plain language of the FOIA; (3) the FOIA's "personal privacy" exemption set forth in West Virginia Code § 29B-1-4(a)(2) is not applicable to documents containing anonymous peer review comments of the draft articles but those documents are still exempt from disclosure under the FOIA's "internal memoranda" exemption; (4) Highland should have been afforded the opportunity to modify its FOIA requests before the circuit court dismissed the action."

The first issue the court addressed was the "internal memoranda" exemption, also known as the 'deliberative process' exemption. W. Va. Code § 29B-1-4(a)(8). The court discussed the importance of this exemption, explaining that without it there may be a "chilling effect… were officials to be judged not on the basis of their final decisions, but for matters they considered before making up their minds." (citations omitted). The court went on to explain that even though WVU, is not an agency engaged in policymaking, the exemption applies. *Id.* The court points out that FOIA applies to *any* public body stating "[w]e hereby announce that West Virginia's Freedom of Information Act, (2012), West Virginia Code § 29B-1-4(a)(8) exempts from disclosure "internal memoranda or letters received or prepared by *any* public body" as defined by West Virginia Code § 29B-1-2(3)."

The court went on to explain that an "academic freedom" privilege cannot circumvent FOIA, and the "personal privacy" exemption did not apply in this case. Finally the court examined whether the requests were reasonable. The lower court had found that the requests proved unreasonable given the large quantity of documents WVU had produced since the initial request. However, the Supreme Court of Appeals of West Virginia pointed out that Highland wished to modify its requests, but was not allowed by the lower court. Therefore the Court allowed Highland to revise its requests on remand at which time the reasonableness would be examined. The court also pointed out that while reasonableness was a factor, FOIA does allow for retrieval of a fee if the request is burdensome. Therefore, courts must be cautious not to use unreasonableness or requests as an easy means for denying State FOIA requests.

Implications:

Public bodies may use the internal memoranda exemption under FOIA even when not engaging in policymaking. Additionally, while courts will consider the burden imposed by a FOIA request, public bodies may establish fees for the cost of

compliance with FOIA (W. Va. Code § 29B-1-3(5)). Therefore it is a high standard of unreasonableness that must be met.

8. *Smith v. Tarr*, No. 13-1230, 2015 WL 148680 (W. Va. 2015).

The plaintiff in *Smith v. Tarr* was a freelance news reporter seeking information regarding ethical judicial violations in West Virginia circuit courts. . In order to obtain that information he sent a West Virginia Freedom of Information Act ("FOIA") request to defendants, the West Virginia Judicial Investigation Commission ("JIC"). His first request was sent in 2012 and then he sent a second on January 31, 2013. The JIC denied the plaintiff's requests, stating the documents were confidential, and cited the confidentiality requirements in the West Virginia Rules of Judicial Procedure[1]. The plaintiff then filed suit against the defendants in the Circuit Court of Kanawha County, asserting that the information sought did not meet a FOIA exemption. The defendants responded, again relying on Rule 2.4 of the West Virginia Rules of Judicial Procedure, and moved to dismiss. The plaintiff responded, arguing that Rule 2.4 violated the West Virginia Constitution. The circuit court found for the defendants and dismissed the complaint.

The Supreme Court of Appeals of West Virginia granted cert and examined the plaintiff's claim that Rule 2.4 is unconstitutional and violates FOIA. Rule 2.4 maintains confidential any "details of complaints filed or investigations conducted" until probable cause is found and a hearing or admonishment occurs at which time the information will be made public. W. Va. Ct. R. 2.4. Because the information sought was for ethical violations that had not resulted in a hearing or admonishment, the plaintiff was requesting confidential information. *Id.* In examining the plaintiff's second claim that Rule 2.4 is unconstitutional as overly broad and for violating FOIA, the Court compared this case to *Charleston Gazette v. Smithers*, 752 S.E.2d 603 (W. Va. 2013). In *Smithers*, a FOIA request was made for records regarding internal reviews of complaints against police officers. *Smithers*, 752 S.E.2d at 608-09. In that case the court found that the records were not exempt. In *Tarr*, the court pointed out that in *Smithers* personal identifying information would be redacted from the FOIA documents, and information regarding ongoing investigation did not need to be released. The Court explained that "public disclosure of governmental records is not limitless." Because the requests were for information that was confidential and there was precedent for limitations on FOIA requests for ongoing investigations, the court found that the plaintiff was not entitled to the information he sought.

Implications:

[1] W. Va. Ct. R. 2.4 Confidentiality ("The details of complaints filed or investigations conducted by the Office of Disciplinary Counsel shall be confidential, except that when a complaint has been filed or an investigation has been initiated, the Office of Disciplinary Counsel may release information confirming or denying the existence of a complaint or investigation, explaining the procedural aspects of the complaint or investigation, or defending the right of the judge to a fair hearing. Prior to the release of information confirming or denying the existence of a complaint or investigation, reasonable notice shall be provided to the judge.").

This State's FOIA are to be liberally construed, and exemptions to the Act are to be strictly construed, citing Syl. Pt. 4, *Hechler v. Casey*, 175 W. Va. 434, 333 S.E.2d 799 (1985). However, there are limitations to this general principle. While the court has previously found that ongoing investigations are exempt, judicial ethical violations are also exempt. While departments still must be aware of the need to respond to FOIA requests specifically and err on the side of disclosure, other state rules and statutes can support a denial of a FOIA request.

B. Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA).

1. *R.K. v. St. Mary's Med. Ctr., Inc*., 229 W. Va. 712, 735 S.E.2d 715 (2012).

In *R.K. v. St. Mary's Med. Ctr., Inc*., the material facts were that while R.K. was in the midst of divorce proceedings, he was admitted to St. Mary's as a psychiatric patient. During his hospitalization, and to further his treatment, R.K. disclosed confidential personal information that he had not previously disclosed to anyone, including his estranged wife. R.K. did not authorize the disclosure of information regarding his psychiatric condition or his hospitalization to his estranged wife or to anyone else. Nevertheless, during R.K.'s hospitalization, St. Mary's employees improperly accessed his medical records, which contained his psychological information, and informed R.K.'s estranged wife and her divorce lawyer of R.K.'s hospitalization and disclosed to them other confidential medical and psychological information pertaining to R.K. After learning of the disclosure, R.K. filed suit against St. Mary's asserting claims for negligence, outrageous conduct, intentional infliction of emotional distress, negligent infliction of emotional distress, negligent entrustment, breach of confidentiality, invasion of privacy, and punitive damages. St. Mary's responded with a motion to dismiss for failure to state a claim pursuant to Rule 12(b)(6) of the West Virginia Rules of Civil Procedure asserting that R.K.'s claims were preempted by HIPAA. Additionally, St. Mary's argued that R.K.'s claims came under the West Virginia Medical Professional Liability Act (MPLA), codified at W. Va. Code § 55-7B-1 *et seq*., and they should, therefore, be dismissed due to his failure to file the required notice of claim and screening certificate of merit required by that Act. The circuit court concluded that HIPAA completely preempted R.K.'s claims and dismissed the suit in its entirety. The circuit court also ruled that R.K.'s claims had not been filed pursuant to the MPLA and, therefore, denied St. Mary's motion to dismiss insofar as it alleged R.K.'s failure to comply the MPLA.

Ruling:

The West Virginia Supreme Court of Appeals held that common-law tort claims based upon the wrongful disclosure of medical or personal health information are not preempted by HIPAA; and that the MPLA West Virginia Medical Professional Liability Act, codified at W. Va. Code § 55–7B–1 *et seq*., applies only to claims resulting from the death or injury of a person for any tort or breach of contract based on health care services rendered, or which should have been rendered, by

a health care provider or health care facility to a patient. It does not apply to other claims that may be contemporaneous to or related to the alleged act of medical professional liability." Syl. Pt. 3, *Boggs v. Camden–Clark Memorial Hospital Corp*., 216 W. Va. 656, 609 S.E.2d 917 (2004).

Implication:

Employers have an obligation to ensure that procedures are in place and followed by their employees so that there is no unauthorized disclosure or use of information that is private under HIPAA or confidential under federal or state law.

2. *Tabata v. Charleston Area Medical Center, Inc.*, 233 W. Va. 512, 759 S.E.2d 459 (2014).

In *Tabata v. Charleston Area Medical Center, Inc.*, the Supreme Court of West Virginia, in a per curium opinion, reversed the circuit court's decision determining that the plaintiffs did not have standing and denying them class certification. The plaintiffs were five of 3,655 patients whose personal information was accidentally posted online by the Charleston Area Medical Center (CAMC). The information included "names, contact details, Social Security numbers, and dates of birth . . . along with certain basic respiratory care information." Upon discovery of the breach, CAMC removed the information, notified the plaintiffs, and offered to pay for a full year of credit monitoring. The plaintiffs filed suit alleging "breach of duty of confidentiality; invasion of privacy—intrusion upon the seclusion of the petitioners; invasion of privacy—unreasonable publicity into the petitioners' private lives; and negligence." Discovery showed that the plaintiffs had not been the victims of any identity theft or suffered any property or economic loss. The circuit court found the plaintiffs lacked standing because the increased risk of future identity theft was a conjectural and hypothetical rather than concrete and particularized injury. In addition, the circuit court denied the plaintiffs' request for class certification because the proposed class lacked commonality, typicality, and the predominance of common issues of law or fact.

Ruling:

In regard to standing, the Supreme Court agreed with the circuit court's contention that "the risk of future identity theft alone [did] not constitute an injury in fact for the purpose of showing standing." However, the court pointed out that West Virginia recognized claims for breach of confidentiality in *Morris v. Consolidation Coal Co.*, 446 S.E.2d 648 (W. Va. 1994): "a patient does have a cause of action for the breach of the duty of confidentiality against a treating physician who wrongfully divulges confidential information." Therefore, the plaintiffs' legal interest in the confidentiality of their medical information leads to a particularized and actual injury when that confidentiality is breached. In addition, the court addressed the claim for invasion of privacy, noting that a "declaration in an action for damages founded on an invasion of the right of privacy ... need not allege that special damages resulted from the invasion." Therefore, since the plaintiffs had alleged an invasion

of their "concrete, particularized, and actual" legal interest in privacy, they did not need to show injury.

In regard to class certification, the court made a rather matter of fact determination that, based on the settled law, the plaintiffs had established commonality, typicality, and the predominance of common issues of law or fact. The court found commonality because there was a "common nucleus of operative fact and law and common issues." It found typicality because the plaintiffs' and proposed class members' claims arose from the same event and were based on the same legal theories. Lastly, although the circuit court found that individual issues of damages and causation would predominate, the court concluded that because no economic injury had been alleged, the class members' similar position would lead to a predominance of common issues of law or fact.

Implications:

The court claims that its holding in this case is narrow, relating only to standing and class certification. However, such a statement fails to appreciate the significance of that narrow holding because it is quite different from other data breach cases. Normally, plaintiffs fail to establish standing in data breach cases because they are unable to show harm that is not conjectural or hypothetical. Although the plaintiffs here could not show any economic harm, their claims for breach of confidentiality and invasion of privacy allowed them to show that there had been a concrete and particularized invasion of their recognized rights. The fact that some form of health data was disclosed is significant because it allowed the plaintiffs to make a claim for breach of confidentiality, a recognized claim in West Virginia for which damages may be recovered. In addition, West Virginia law allows a claim for invasion of privacy to be maintained whether or not the plaintiff can allege special damages. Although the merits of the case have yet to be decided, it is clear that the Supreme Court views the disclosure of personal information, including health data, to be an actionable tort under breach of confidentiality and invasion of privacy.

Note: In *Mays v. Marshall Univ. Bd. of Governors*, No. 14-0788, 2015 WL 6181508 (W. Va. Oct. 20, 2015), the Supreme Court of Appeals of West Virginia distinguished *Tabata* in a case where medical information was disclosed to two people at the plaintiffs' work rather than the public at-large.

In *Byrne v. Avery Ctr. for Obstetrics and Gynecology*, the Supreme Court of Connecticut examined whether HIPAA preempts state negligence claims for breach of patient privacy. 102 A.3d 32 (Conn. 2014). The cause of action arose after the defendant provided the plaintiff's medical records to a state court pursuant to a subpoena for use in a paternity suit. The plaintiff previously advised the defendant not to release her medical records to her significant other who filed the paternity suit. Despite the plaintiff's instructions, the defendant provided the records without notifying the plaintiff, filing a motion to quash the subpoena, or appearing in court. The plaintiff sued the defendant for failure to use reasonable

care in protecting her medical information, including making disclosures in violation of HIPAA. The lower court dismissed the claims ruling that because HIPAA does not provide for a private right of action, the plaintiff could not assert negligence claims against the defendant based on HIPAA noncompliance. The Connecticut Supreme Court overturned the lower court's decision, holding instead that a plaintiff may use HIPAA to establish the standard of care in negligence cases. The court recognized that HIPAA does not grant a private right of action, but also concluded that state causes of action are not preempted solely because they impose liability over and above that authorized by federal law. The court's ruling provides that HIPAA may be used to inform the standard of care to the extent that HIPAA has become the common practice for Connecticut health care providers.

In *Jackson v. Mercy Behavioral Health*, the Western District of Pennsylvania examined whether an individual can state a claim for a HIPAA violation. No. 14-1000, 2015 WL 401645 (W.D. Pa. Jan. 28, 2015). The plaintiff in that case was a patient at the defendant hospital in a "30 day residential program to divert consumers from inpatient psychiatric care." The defendant allegedly faxed confidential medical information to the plaintiff's dentist, and then informed the plaintiff that if she did not sign a consent to release information form she would be discharged from the program early. She refused to sign and was discharged three days early. The plaintiff then brought suit, alleging violation of HIPAA and unlawful retaliation. The court found that HIPAA violations are under the exclusive jurisdiction of the Department of Human Service and the Office for Civil Rights, and as such the court did not have subject matter jurisdiction over the claim. Because of the absence of a state tort claim, she did not claim a cause of action the court could hear.

See also Murphy v. Dulay, 768 F.3d 1360 (11th Cir. 2014) (finding that HIPAA does not preempt a Florida pre-suit requirement that a written authorization form for release of PHI be signed before an individual may bring suit for medical negligence).

3. *W. Va. Dep't of Health & Human Res. v. E.H.*, 236 W. Va. 279, 778 S.E.2d 728 (2015)

This case arose from an order of the Circuit Court of Kanawha County directing the DHHR to restore access to patients and medical records to patient advocates from West Virginia Legal Aid. The underlying litigation concerned conditions at two psychiatric hospitals. Pursuant to an order from the West Virginia Supreme Court, the DHHR contracted with Legal Aid to provide patient advocacy services. The DHHR also created the Office of the Ombudsman which was charged with overseeing compliance related to the operation of the hospitals. A court-approved agreement in 2009 led to DHHR contracting again with Legal Aid to produce a report for the court on the progress of implementation of state regulations. After more than a decade of access, the DHHR began requiring patient advocates to obtain signed releases from each patient (or the person's guardian or other legal

custodian) before each time the advocate wished to review the patient's records. Legal Aid filed a motion for emergency relief which the circuit court granted in 2014.

Ruling:
The West Virginia Supreme Court of Appeals affirmed the circuit court's decision to restore Legal Aid's patient access to the level it experienced prior to the June 2014 policy change.

The court rejected the DHHR's argument that the access afforded to Legal Aid prior to the policy change violated patients' constitutionally-based rights of privacy. Instead, the Court found that because the record failed to demonstrate any indiscriminate disclosure of confidential information by Legal Aid, no meritorious issue existed with regard to its dissemination of confidential health information.

Turning next to HIPAA considerations, the court agreed with the DHHR's argument that Legal Aid does not come within any exemptions provided under HIPAA that would eliminate its need to obtain patient consent before viewing medical records. Specifically, the court disagreed with the circuit court's determination that Legal Aid falls within the HIPAA definitions for a "business associate," a "health oversight agency," or "health care operations." Rather, the court held that no exemption of HIPAA entitled Legal Aid to records without patient consent.

Having determined that federal law does not provide the necessary authority for disclosure of patient records to Legal Aid without express written consent, the court turned to state law (specifically, Title 64, Series 59 of the Code of State Regulations governing "Behavioral Health Patient Rights" pursuant to W. Va. Code § 27-5-9) to determine whether it provided an independent basis to support the circuit court's ruling. West Virginia law provides that while a patient may authorize the release of his or her medical records, those records may also be obtained by the "providers of health, social, or welfare services involved" in caring for a patient. State law further provides that "[n]o written consent is necessary for . . . advocates under contract with" the department serving the patient.

The court held that the written agreement between the DHHR and Legal Aid specifying the legal obligations of the parties (including the manner of payment and the duties associated with the provision of patient advocacy services) constitutes a contract for purposes of permitting Legal Aid to access records without written consent of individuals hospitalized in state mental health facilities. The court further held that the contract falls within the meaning of the state regulation permitting disclosure of patient records without written consent under contract. Accordingly, the court affirmed the circuit court's ruling that the DHHR's revocation of Legal Aid's access to patient records violates state law.

In addition, the court found that the policy adopted by the DHHR is not preempted by HIPAA because the state's laws are more stringent than those set forth in HIPAA, consistent with the findings of West Virginia's HIPAA Preemption Analysis.

Finally, the court affirmed the circuit court's order restoring Legal Aid's access to the hospitals' patients without limitation, except when patients expressly request limitations on the disclosure of their identifiable health information. The court identified a clear need for periodic review of patient records to identify systemic issues of noncompliance with state regulations and noted the court-approved agreement's requirement for a report to the judge on such issues.

In dissent, Justice Davis agreed with the majority that Legal Aid could not find support through HIPAA. She disagreed, however, that state law provided a haven. Justice Davis found the majority's preemption analysis insufficient and that giving Legal Aid unfettered access to patient records did not afford the greater privacy protections required to find state law more stringent than HIPAA regulations.

The DHHR submitted a Petition for Writ of Certiorari to the United States Supreme Court in March, 2016. The United States Supreme Court denied the Petition for Writ of Certiorari on October 11, 2016. (See Docket No. 15-1142)

Implications:
When analyzing contractual relationships involving disclosure of or providing access to patient records, Departments should determine the relationship between the parties through an independent legal analysis. This analysis should determine whether the disclosure or access contemplated by the contract triggers any federal laws such as HIPAA, or state laws, including the West Virginia Code and the Code of State Regulations. Departments may consult the West Virginia HIPAA Preemption Analysis published annually as educational guidance to assist in making a determination as to whether the state or federal law is applicable with respect to the contract. The legal analysis should also include a formal preemption determination. Finally, legal counsel should establish whether the disclosure of or access to patient records complies with an exception that permits disclosure or access without patient authorization, or whether patient authorization is required.

C. Federal Telephone Consumer Protection Act (TCPA)

1. *Mey v. Pep Boys-Manny*, 228 W. Va. 48, 717 S.E.2d 235 (2011).

In *Mey v. Pep Boys-Manny*, the defendants had left an automated voicemail message at plaintiff's residence in response to a classified advertisement that the plaintiff's son placed on the internet website craigslist.com. The plaintiff's son was selling a used car and his internet advertisement invited third parties to contact him at the plaintiff's home telephone number. The defendant responded to the advertisement by leaving an automated message on the plaintiff's answering machine. After receiving this message, the plaintiff filed a class action complaint against three defendants, The Pep Boys, Lanelogic Inc., and Southwest Vehicle Management Inc., who allegedly entered into a partnership to purchase used cars. The plaintiff sought damages and an injunction under the Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227, to redress the alleged harm caused by

the automated message left on her answering machine. The circuit court ruled that the automated call placed in response to this advertisement did not violate the TCPA and granted the defendants' motion to dismiss. The Supreme Court of Appeals affirmed the decision of the circuit court.

Ruling:
The West Virginia Supreme Court of Appeals held the under the Federal Telephone Consumer Protection Act a caller responding to a classified advertisement is not making a "telephone solicitation" in violation of the Act, provided the purpose of the call is to inquire about or offer to purchase the product or service advertised, rather than to encourage the advertiser to purchase, rent, or invest in property, goods, or services.

2. *Moore v. Dish Network*, 57 F. Supp. 3d 639 (N.D. W. Va. 2014).

In *Moore v. Dish Network*, the plaintiff applied for a cell phone that was subsidized through the Federal Lifeline Program from Cintrex Wireless, while having a subsidized cell phone through another program. After receiving the new cell phone, Moore began receiving phone calls from DISH network regarding a past due account, despite the fact that Moore was not and had never been a DISH customer. Moore informed DISH several times that he was not a customer and DISH was calling the wrong number, but he received 31 automated calls from DISH network between January and August, 2012. DISH added Moore to a do-not-call list on June 11, 2012, but he received multiple calls after that date. Moore then brought suit under the Telephone Consumer Protection Act (TCPA).

Ruling:
DISH network made several arguments against Moore. The first was that Moore could not bring suit because he violated the federal Lifeline program by having two subsidized phones. The Northern District of West Virginia found that the TCPA does concern itself with how a phone was obtained, and there was not a strong public policy supporting dismissal, so Moore's case was not barred on those grounds. *Id.* at 645. The second argument by DISH was that recovery cannot be had under the TCPA if the individual is not charged for the calls. *Id.* After examining the language of the TCPA the court found that the language that required being charged only modified that part of the sentence, and therefore being charged is not a requirement of the TCPA. Dish then argued that because Moore was not the "called party" he could not bring suit. The court found that the TCPA does not limit standing to only a "called party," and is not limited only to the intended recipient of the calls. While DISH attempted a few other arguments, the court found that Moore had standing, and awarded him treble damages for all calls after the attempt to put him on a do-not-call list.

6.0. Payment Card Industry Data Security Standards (PCI DSS)

Description:

The Payment Card Industry Data Security Standards (PCI DSS) are published by the PCI Security Standards Council (the Council). The Council was founded jointly by American Express, Discovery Financial Services, JCB International, MasterCard, and Visa Inc. These industry standards are not law, but have been developed by the above credit card companies to create a single set of requirements for consumer data protection. Enforcement of compliance and determination of non-compliance penalties is carried out by each individual payment brand that has decided to incorporate PCI DSS as its technical requirements for data security.

The PCI DSS specifically identify that credit card companies should protect stored data, encrypt transmission of cardholder data and sensitive information across public networks, and maintain a policy that addresses information security. PCI DSS applies to all members of the PCI Security Standards Council, merchants, and service providers that store, process, or transmit cardholder data. Additionally, these security requirements apply to all "system components" which are defined as any of the following:

- Network Components, which include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances;
- Servers, which include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP; and
- Applications included in, or connected to, the cardholder data environment (this includes all purchases and custom applications, including internal and external web applications).

In October, 2010 the Council published two whitepapers concerning PCI DSS. The first, titled "PCI DSS Applicability in an EMV Environment," discussed PCI DSS in the wider framework of the global standard established by Europay, Mastercard, and Visa which use integrated circuit cards (aka smart cards) to enhance security. However, while EMV stands to improve security, no action is required from the State as the EMV environment today does not in all cases fulfill PCI DSS requirements or protect cardholder confidentiality and sensitive authentication data. The second white paper, "Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance" covered P2PE (point-to-point encryption) as a means to simplify PCI DSS compliance standards. It found that implementation of P2PE was "immature" and that standardization would be needed before consistent security practices could be realized.

In March, 2011, the Council issued an information supplement titled "Protecting Telephone-based Payment Card Data" (the "Supplement"); it does not replace or supersede any PCI DSS requirements but is only intended to provide supplemental

guidance. The Supplement provides information and guidance for merchants and service providers (i.e. call centers) who accept and/or process payment card data over the telephone; specifically clarifying the requirements as to voice recordings and what Sensitive Authentication Data may be maintained and what should be destroyed. Then in September 2011, the Council issued the Report on Compliance (ROC) as guidance to assessors to ensure that a proper and consistent level of reporting is maintained.

In November 2013, the Council published Version 3.0 of the PCI DSS, which went into effect on January 1, 2014. In April, 2015, the Council published Version 3.1 of the PCI DSS, which supplements Version 3.0. Much like prior versions, Version 3.1 involves a great deal of clarification, additional guidance, and enhancement concerning existing requirements. However, Version 3.1 also implements far more "evolving requirements" than previously seen. Some of the new requirements are as follows:

- Maintain an inventory of system components that are in scope for PCI DSS to support development of configuration standards;
- Evaluate evolving malware threats for any systems not considered to be commonly affected by malicious software;
- Ensure that anti-virus solutions are actively running and cannot be disabled or altered;
- Protect against broken authentication and session management with coding practices (effective July 1, 2015);
- Use of unique authentication credentials for each customer for service providers with remote access to customer premises;
- Ensure only intended user can gain access with authentication mechanisms linked to an individual account;
- Control physical access to sensitive areas for onsite personnel;
- Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution (effective July 1, 2015);
- Implement a methodology for penetration testing (effective July 1, 2015);
- Perform penetration tests to verify that segmentation methods are operational and effective if used to isolate the CDE from other networks;
- Implement a process to respond to any alerts generated by the change-detection mechanism; and
- Maintain information about which PCI DSS requirements are managed by each service provider and which are managed by the entity.

Version 3.2 was released in April 2016. Because PCI DSS is now a mature standard, version 3.2 sought to clarify requirements. Among the changes included sunset dates for Revised Secure Sockets Layer and early Transport Layer

Security, expansion of multi-factor authentication for personnel with administrative access, and additional security validation steps for service providers and others.

Source:

PCI Security Standards Council website
https://www.pcisecuritystandards.org/

PCI DSS Version 3.1
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

Summary of Changes from PCI DSS Version 3.0 to 3.1
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1_Summary_of_Changes.pdf

PCI DSS Version 3.2
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1469745408401

Summary of Changes from PCI DSS Version 3.1 to 3.2
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_Summary_of_Changes.pdf?agreement=true&time=1469745408498

PCI SSC Data Security Standards Overview
https://www.pcisecuritystandards.org/pci_security/standards_overview

Best Practices:

- Build and maintain secure computer networks and applications.
- Protect cardholder data.
- Limit access.
- Respond quickly and efficiently to incidents.
- Be aware and protect against the latest threats regarding credit card use and stored data.
- If payments are received by phone and if those calls are recorded, then technology should be used to delete or prevent the recordation or the recovery of Sensitive Authentication Data from those recordings.

Principles:

Security Safeguards, Accountability, Minimum Necessary and Limited Use