STATE OF WEST VIRGINIA

EXECUTIVE DEPARTMENT

At Charleston

EXECUTIVE ORDER NO. 3-17

By the Governor

WHEREAS, our interconnected digital world has created the need to proactively protect information systems and sensitive information entrusted to the State of West Virginia (the "State"); and

WHEREAS, safeguarding the privacy of personal information collected, used, disclosed and maintained by the State is of the utmost importance to the citizens of the State; and

WHEREAS, the United States Congress has enacted laws protecting the privacy of citizens' personally identifiable information, including protected health information, including the Privacy Act of 1974, Public Law 93-579, the CAN-SPAM Act of 2003, Public Law 108-187, and the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191; and

WHEREAS, pursuant to West Virginia Code §5A-6-4, the Chief Technology Officer in the Department of Administration (the "CTO") is responsible for leading cyber security efforts designed to provide reasonable information security through empowering the State's adoption, integration, and protected use of technology; and

WHEREAS, pursuant to Executive Order No. 7-03, the Privacy Management Team was formed to develop privacy protections for state government and the Chair of the West Virginia Health Care Authority ("HCA") sponsored the Privacy Management Team; and

WHEREAS, Executive Order No. 6-06 rescinded and superseded Executive Order No. 7-03, and pursuant to Executive Order No. 6-06, the HCA Chair is responsible for developing and overseeing the State's Privacy Program (the "Privacy Program") for all Executive Branch

department-level organizations, including creating and maintaining a Privacy Team comprised of representatives from all Executive Branch department-level organizations with appropriate staff, support, management and leadership; and

WHEREAS, the Legislature enacted House Bill 2459, relating to regulation of health care and the certificate of need process, during the 2017 regular legislative session, which transfers the direct supervision of the HCA to the Secretary of the Department of Health and Human Resources; and

WHEREAS, pursuant to West Virginia Code §5A-6-4, the CTO is responsible for an enterprise cyber security strategy, policy and standards, designed to leverage a risk management approach and establish clear roles and responsibilities through outlined governance; and

WHEREAS, pursuant to West Virginia Code §29-12-5, the Board of Risk and Insurance Management ("BRIM") is responsible for providing reasonably broad protection against loss, damage or liability to state property and on account of State activities, through methods of protection and principles of loss control and risk; and

WHEREAS, BRIM is responsible for administering the cyber-liability insurance policy for the State, the benefits of which are available to all Executive Branch state agencies and other insureds; and

WHEREAS, BRIM has developed and implemented a program to assist its insureds with risk mitigation strategies in the areas of privacy and cyber liability and has the expertise to identify data privacy risks and proactively protect sensitive information, and oversee, support and manage the State's Privacy Program including maintaining the State Privacy Office and the State's existing Privacy Management Team; and

WHEREAS, it is imperative that the State actively engage with its business partners to appropriately safeguard the privacy of all West Virginians.

NOW, THEREFORE, I, JIM JUSTICE, by virtue of the authority vested in me as the Governor of the State of West Virginia, do hereby **ORDER** that:

1. Executive Order No. 6-06 is hereby rescinded and superseded.
2. The Director of BRIM (the "Director") shall be responsible for protecting the privacy of personally identifiable information, including protected health information, collected and maintained by Executive Branch agencies.
3. The CTO shall be responsible for conducting cyber risk management oversight activities, assisting agency heads in the identification, analysis and decision-making process key to ensuring appropriate cyber security protections.
4. The Director is hereby empowered to oversee the State's Privacy Program and to:
    a. Maintain the State Privacy Office to lead and manage the Privacy Program; and
    b. Maintain a Privacy Management Team comprised of appointed representatives from all Executive Branch department-level organizations, to inform strategy and advance governance, with appropriate staff support, management and leadership; and
    c. Issue privacy policies applicable to all Executive Branch department-level organizations; and
    d. Continue to provide privacy awareness to the Executive Branch workforce; and
    e. Conduct privacy assessments.
5. All tangible personal property, including equipment, furniture and other necessary materials used by HCA to support the Privacy Program shall be transferred to the Director.
6. The CTO is hereby empowered to develop and oversee a Cyber Security Program and to:
    a. Maintain a Cyber Security Team comprised of appointed representatives from all Executive Branch department-level organizations, to inform strategy and advance governance, with appropriate staff support, management and leadership; and

b. Create technology focused workgroups to conduct cyber security training, education, collaboration and information sharing; and

c. Issue cyber security policies and baselines indicating minimum levels of cyber security protection applicable to all Executive Branch department-level organizations; and

d. Conduct or oversee cyber security risk assessments.

7. The Privacy Program shall balance individuals' rights of privacy against others' need and right of access to personally identifiable information. The Director shall continuously evaluate the Privacy Principles that guide the Privacy Program in its work.

8. The CTO shall continuously evaluate the Cyber Security Principles that guide the Cyber Security Program in its work.

9. The Director shall submit a report on the work of the Privacy Program to the Governor prior to the first day of each calendar year.

10. The CTO shall submit a report on the work of the Cyber Security Program to the Governor prior to the first day of each calendar year.

IN WITNESS WHEREOF, I have hereunto set my hand and caused the Great Seal of the State of West Virginia to be affixed.

DONE at the Capitol, in the City of Charleston, State of West Virginia, this eighteenth day of May, in the year of our Lord, Two Thousand Seventeen, and in the One Hundred Fifty-Fourth year of the State.

GOVERNOR

By the Governor

SECRETARY OF STATE