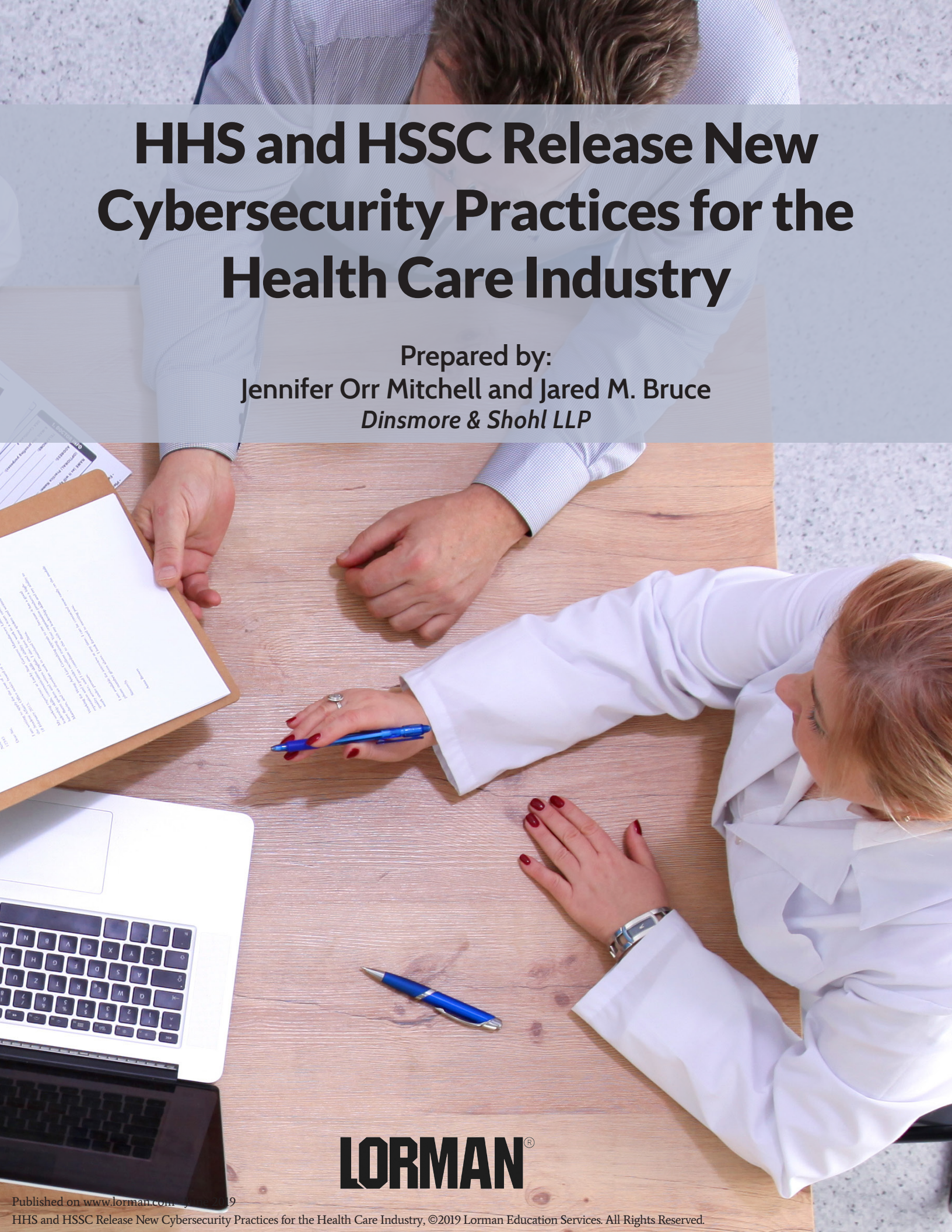

HHS and HSSC Release New Cybersecurity Practices for the Health Care Industry

Prepared by:
Jennifer Orr Mitchell and Jared M. Bruce
Dinsmore & Shohl LLP

LORMAN®

Published on www.lorman.com

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

HHS and HSSC Release New Cybersecurity Practices for the Health Care Industry

Written by Jennifer Orr Mitchell and Jared M. Bruce – 1/31/19

On December 28, 2018, the Department of Health and Human Services (HHS), in partnership with the Health Sector Coordinating Council (HSSC), published the "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" (HICP Publication), which is a four-volume publication designed to provide voluntary cybersecurity practices to health care organizations of all types and sizes, ranging from local clinics to large health care systems. The HICP Publication was in response to a mandate set forth by the Cybersecurity Act of 2015, Section 405(d), to develop practical cybersecurity guidelines to cost-effectively reduce cybersecurity risks for the health care industry. HHS and HSSC led a task group, comprised of cybersecurity industry leaders, to develop the HICP Publication. All health care organizations should review and consider the implementation of the recommendations set forth in the HICP Publication.

The main document of the HICP Publication explores the five most relevant and current threats to the health care industry. It also recommends 10 cybersecurity practices to help mitigate these threats. The main document presents real-life events and statistics that demonstrate the financial and patient care impacts of cyber incidents. Moreover, the HICP Publication also lays out a call to action for all industry stakeholders that protective and preventive measure must be taken now.

HHS notes the process of implementing cybersecurity practices is not a one-size fits all approach. The complexity of an organization's cybersecurity needs will increase or decrease based upon that organization's specific characteristics and the nature of products and/or services provided. Therefore, the HICP Publication also includes two technical volumes geared for IT and IT security professionals based upon the size of the health care organization. Technical Volume 1 focuses on cybersecurity practices for small health care organizations, while Technical Volume 2 focuses on practices for medium and large health care organizations. The last volume of the HICP Publication provides resources and templates organizations can leverage to assess their cybersecurity posture, as well as develop policies and procedures.

Five Most Current Cybersecurity Threats to the Industry

The main document of the HICP Publication classifies the following as the most current cybersecurity threats to the health care industry and provides examples of cybersecurity practices that can minimize these threats. The HICP Publication examines the vulnerabilities, impact and practices to consider regarding each threat.

1. **E-mail phishing attacks**

An e-mail phishing attack is an attempt to trick an e-mail recipient into giving out information using e-mail. It occurs when an attacker, posing as a trusted party (such as a friend, co-worker, or business partner), sends a phishing e-mail that includes an active link or file (often a picture or graphic). When the e-mail recipient opens the link, the recipient is taken to a website that may solicit sensitive information, proactively infect the computer, or compromise the organization's entire network. Accessing the link or file may result in malicious software being downloaded or access being provided to information stored on the recipient's computer or other computers within the organization's network.

According to the HICP Publication, the lack of IT resources for managing suspicious e-mails, lack of software scanning e-mails for malicious content or bad links, and lack of e-mail detection software for testing malicious content, or e-mail sender and domain validation tools, are vulnerabilities that can expose a health care organization to the phishing threat. E-mail phishing attacks can adversely impact a health care organization by causing a loss of reputation in the community, result in stolen access credentials, create an erosion of trust or brand reputation, and potentially impact the ability to provide timely and quality patient care, which could lead to patient safety concerns.

The HICP Publication recommends health care organizations consider adopting the following practices to protect against e-mail phishing attacks:

- Be suspicious of e-mails from unknown senders; e-mails that request sensitive information, such as protected health information (PHI) or personally identifiable information (PII); or e-mails that include a call to action that stresses urgency or importance.
- Train staff to recognize suspicious e-mails, know where to forward them, and never open e-mail attachments from unknown senders.
- Implement the following:
    - Incident response plays to manage successful phishing attacks;
    - Advanced technologies for detecting and testing e-mail for malicious content or links;
    - Multifactor authentication; and
    - Proven and tested response procedures when employees click on phishing e-mails.
- Establish cyber threat information sharing with other health care organizations.

2. **Ransomware attack**

HHS defines ransomware as "a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid."[1] Most ransomware attacks are sent in phishing campaign e-mails asking the recipient to either open an attachment or click on an embedded link. After a user's data is encrypted, the ransomware will direct the user to pay the ransomware to the hacker, typically

in cryptocurrency, in order to receive a decryption key to release the data. Paying the ransom does not guarantee the hacker will unencrypt or unlock the stolen or locked data.

According to the HICP Publication, the lack of system backup, lack of anti-phishing capabilities, unpatched software, lack of anti-malware detection and remediation tools, lack of testing and proven data backup and restoration, and lack of network security controls, such as segmentation and access control, are vulnerabilities that may result in an organization's exposure to ransomware. Ransomware attacks can adversely impact a health care organization by resulting in partial or complete clinical and service disruption, patient care and safety concerns, and expenses for recovery from a ransomware attack. Moreover, it is important to note the presence of ransomware (or any malware) on a covered entity's or business associate's computer system is a security incident under the HIPAA Security Rule, and the covered entity or business associate must initiate its security response reporting procedures.[2]

The HICP Publication recommends health care organizations consider adopting the following practices to protect against ransomware attacks:

- Ensure users understand authorized patching procedures and patch software according to authorized procedures.
- Specify which computers may access and store sensitive or patient data.
- Use strong/unique username and passwords with multifactor authentication.
- Limit users who can log in from remote desktops and the rate of allowed authentication attempts to thwart brute-force attacks.
- Deploy anti-malware detection and remediation tools.
- Separate critical or vulnerable systems from threats.
- Maintain a complete and updated inventory of assets.
- Implement a proven and tested data backup and restoration test and proven and tested incident response procedures. Backups should be secured so they are not accessible on the network they are backing up.
- Establish cyber threat information sharing with other health care organizations.

3. **Loss or theft of equipment or data**

The HICP Publication notes that every day, mobile devices, such as laptops, tablets, smartphones, and USB/thumb drives, are lost or stolen and may end up in the hands of hackers. HHS notes from January 1, 2018, to August 31, 2018, the Office for Civil Rights received reports of 192 theft cases affecting 2,041,668 individuals. When lost equipment is not appropriately safeguarded or password protected, the loss may result in unauthorized or illegal access, dissemination, and use of sensitive data.

According to the HICP Publication, vulnerabilities that can lead to the loss or theft of equipment or data include:

- Lack of asset inventory and control;
- Failure to encrypt data at rest;
- Lack of physical security practices, including open office and poor physical management;
- Lack of simple safeguards, such as computer cable locks to secure devices;
- Lack of effective vendor security management, including controls to protect equipment or sensitive data; and
- Lack of "End-of-Service" process to clear sensitive data before IT assets, including medical devices, are discarded or transferred to other users or other organizations.

Loss or theft of equipment or data may adversely impact a health care organization by resulting in inappropriate access to or loss of sensitive information, including proprietary or confidential information or intellectual property. Moreover, theft or loss of unencrypted PHI or PII may occur, which could result in a data breach requiring notification to impacted individuals, regulatory agencies, and media outlets. Additionally, the health care organization's reputation could be severely damaged.

The HICP Publication recommends health care organizations consider adopting the following practices to protect against the loss or theft of equipment or data:

- Encrypt sensitive data, especially when transmitting data to other devices or organizations. Encrypt data at rest on mobile devices to be inaccessible to anyone who finds the device.
- Implement proven and tested data backups, with proven and tested restoration of data, and implement a safeguards policy for mobile devices supplemented with ongoing user awareness training on securing these devices.
- Acquire and use data loss prevention tools.
- Promptly report loss/theft to designated company individuals to terminate access to the device and/or network.
- Maintain a complete, accurate, and current asset inventory to mitigate threats, especially the loss and theft of mobile devices, such as laptops and USB/thumb drives.
- Define a process with clear accountabilities to clean sensitive data from every device before it is retired, refurbished, or resold.

4. **Insider, accidental or intentional data loss**

Insider threats exist within every health care organization when employees, contractors, or other users access the organization's technology infrastructure, network, or databases. HHS has placed insider threats into two groups: accidental insider threats and intentional insider threats. An accidental insider threat is unintentional loss caused by honest mistakes, like being tricked, procedural errors, or a degree of negligence. For example, being the victim of an e-mail phishing attack is an accidental insider threat. An intentional insider threat is

malicious loss or theft caused by an employee, contractor, or other user of the organization's technology infrastructure, network, or databases, with an objective of personal gain or inflicting harm to the organization or another individual.

According to the HICP Publication, health care organizations are vulnerable to insider data loss when:

- Files containing sensitive data are accidentally e-mailed to incorrect or unauthorized addressees;
- There is a lack of adequate monitoring, tracking, and auditing of access to patient information on electronic health record systems;
- There is a lack of adequate logging and auditing of access to critical technology assets, such as e-mail and file storage;
- There is a lack of technical controls to monitor the e-mailing and uploading of sensitive data outside the organization's network; and
- There is a lack of physical access controls or training about social engineering and phishing attacks.

Insider data loss can result in reportable data breaches and incidents when the accidental loss of PHI or PII occurs through e-mail and unencrypted mobile storage. Moreover, reportable incidents can occur when employees inappropriately view patient information. Financial loss can occur because of insiders who are socially engineered into not following proper procedures and due to employees who give access to banking accounts and routing numbers after falling victim to phishing e-mail attacks disguised as bank communications.

The HICP Publication recommends health care organizations consider adopting the following practices to prevent accidental insider or intentional insider data loss:

- Train staff and IT users on data access and financial control procedures to mitigate social engineering or procedural errors.
- Implement and use the following;
    - Workforce access auditing of health record systems and sensitive data;
    - Privileged access management tools to report access to critical technology infrastructure and systems; or
    - Data loss prevention tools to detect and block leakage of PHI and PII via e-mail and web uploads.

5. **Attacks against connected medical devices that may affect patient safety**

The Food and Drug Administration (FDA) defines a medical device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them;

intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease."[3] The HICP Publication notes a hacker may attempt to gain access to a health care provider's network to take control of a connected medical device to put patients at risk.

HHS notes connected medical devices can be vulnerable if software patches are not implemented promptly, including regular and routine commercial system patches to maintain medical devices, or when legacy equipment is used that is outdated and lacks current functionality. Moreover, according to HHS, connected medical devices, unlike IT equipment, cannot be monitored by an organization's intrusion detection system (IDS). As a result, the safety of patients and protection of data integrity are dependent on identifying and understanding the threats and threat scenarios. However, it is the challenge of identifying and addressing vulnerabilities in medical devices that augments the risk of threats compared with managed IT products. For medical devices, the cybersecurity profile information is not readily available at health care organizations, making cybersecurity optimization more challenging. This may translate into missed opportunities to identify and address vulnerabilities, increasing the likelihood for threats to result in adverse effects.

Compromised connected medical devices have broad implications to health care organizations, because medical devices may be entirely unavailable or will not function properly, compromising patient safety.

The HICP Publication recommends health care organizations consider adopting the following practices to safeguard from attacks against connected medical devices:

- Establish and maintain communication with the connected medical device manufacturer's product security teams.
- Patch devices after patches have been validated, distributed by the medical device manufacturer, and properly tested.
- Assess current security controls on networked medical devices and inventory traits such as IT components that may include the Media Access Control (MAC) address, Internet Protocol (IP) address, network segments, operating systems, applications, and other elements relevant to managing information security risks.
- Implement the following:
    - Pre-procurement security requirements for vendors;
    - Information security assurance practices, such as security risk assessments of new devices and validation of vendor practices on networks or facilities;
    - Access controls for clinical and vendor support staff, including remote access, monitoring of vendor access, multifactor authentication, and minimum necessary or least privilege; and
    - Security operations practices for devices, including hardening, patching, monitoring, and threat detection capabilities.

- Engage information security as a stakeholder in clinical procurements.
- Use a template for contract language with medical device manufacturers and others.
- Develop and implement network security applications and practices for device networks.

10 Cybersecurity Practices to Minimize Threats

The HICP Publication includes two volumes that provide specific cybersecurity practices geared for IT security professionals split between a volume for small health care organizations and medium to large health care organizations (HICP Technical Volumes). Among other criteria, the HICP Publication classifies a "small health care organization" as an organization that has one to 10 physicians, one or two health information exchange partners, and one practice or care site. Medium to large health care organizations have 26 to more than 500 providers, include multiple sites in a very extended geographic area, and have a significant number of health information exchange partners. Both HICP Technical Volumes provide general cybersecurity practices to address the five most relevant cybersecurity threats to health care organizations. Each general cybersecurity practice is then divided among specific sub-practices that address the technical components needed to implement the cybersecurity practices. HICP has recommended a total of 88 specific sub-practices for organizations to consider in their cybersecurity framework.

1. **E-mail protection systems**

Health care organizations are often targeted through e-mail attacks. As a result the HICP Technical Volumes recommend the following practices be adopted to protect e-mail systems. E-mail systems should be configured to ensure controls are in place to enhance security posture. Small health care organizations should check with their e-mail service provider to ensure controls are in place or enabled. The HICP Technical Volumes recommend "free" or "consumer" e-mail systems be avoided, as such systems are not approved to store, process, or transmit PHI. Alternatively, it is suggested health care organizations contract with a service provider that caters to the health care sector. Workforce education and training programs that include sections on phishing and recognition of phishing techniques should be implemented.

The HICP Technical Volumes recommend larger health care organizations consider advanced threat protection services that provide protection against phishing attacks and malware, implement digital signatures that allow the sender to cryptographically sign and verify e-mail messages, and use data analytics to determine the most frequently targeted users in an organization. Additionally, larger health care organizations should have more robust education programs that include ongoing simulated phishing campaigns, ongoing and targeted training, newsletters, and recurring departmental meetings regarding information security.

2. **Endpoint protection systems**

The HICP Technical Volumes recommend endpoints such as desktops, laptops, mobile devices and other connected hardware devices (e.g., printers and medical equipment) be protected. Smaller health care organizations should implement basic endpoint controls, such as:

- Removing administrative access accounts for all users and limiting administrative access to limited number of users;
- Regularly updating systems to remove vulnerabilities that can be exploited by attackers;
- Antivirus software;
- Endpoint encryption;
- Firewalls; and
- Multifactor authentication for remote access.

Larger health care organizations should take more precautions, including implementing basic endpoint controls such as:

- Antivirus software that can detect known malicious malware using signatures, heuristics, and other techniques;
- Full disk encryption, which encrypts the entire disk to make it unreadable for unauthorized individuals;
- Configuration of the endpoint operating system in the most secure manner possible, limiting the usage of local administrator accounts, enabling local firewalls, limiting inbound access to the endpoint to only required ports, and disabling unnecessary services and programs;
- A process ensuring regular patching of endpoint OS and third-party application;
- Provisioning of privileged access to users for installing or updating application and OS software; and
- Mobile device management technologies to manage the configuration of devices and offer application management and containerization.

3. **Identity and access management**

The HICP Technical Volumes recommend health care organizations of all sizes clearly identify all users and maintain audit trails that monitor each user's access to data, applications, systems, and endpoints. According to the HICP Technical Volumes, organizations of all sizes should implement an Identity and Access Management (IAM) program, which is a program that encompasses the processes, people, technologies, and practices relating to granting, revoking, and managing user access. The HICP Technical Volumes note that given the complexities associated with health care environments, IAM models are critical for limiting the security vulnerabilities that can expose organizations.[4] Basic access authentication methods rely on usernames and passwords, a model proven by the success of phishing and hacking attacks to be weak. The HICP Technical Volumes recommend stronger authentication

methods, such as passphrases, and limiting the rate at which authentication attempts can occur to severely restrict the ability of automated systems to brute force the password.

4. **Data protection and loss prevention**

The HICP Technical Volumes recommend all health care organizations establish a data classification policy that categorizes data (e.g., Highly Sensitive, Sensitive, Internal Use, or Public Use) and identify the types of records relevant to each category. For example, the "Sensitive Data " category should include PHI, social security numbers (SSNs), credit card numbers, and other information that must comply with regulations, may be used to commit fraud, or may damage the organization's reputation. After the data has been classified, procedures can be written that describe how to use these data based on their classification. The HICP Technical Volumes recommend the health care organization's workforce be trained to comply with organizational policies and at a minimum, annual training be provided regarding the use of encryption and PHI transmission restrictions.

5. **Asset management**

The HICP Technical Volumes suggest health care organizations with effective cybersecurity practices manage IT assets using processes referred to collectively as IT asset management (ITAM). It is recommended ITAM processes be implemented for all endpoints, servers, and networking equipment for loss prevention. ITAM processes enable organizations to understand their devices and the best options to secure them. The HICP Technical Volume notes while it can be difficult to implement and sustain ITAM processes, such processes should be part of daily IT operations and encompass the lifecycle of each IT asset, including procurement, deployment, maintenance, and decommissioning (i.e., replacement or disposal) of the device.

6. **Network management**

The HICP Technical Volumes state an effective network management strategy includes the deployment of firewalls to enable proper access inside and outside of the organization. Firewall technology is far more advanced than standard router-based access lists and is a critical component of modern network management. The HICP Technical Volumes recommend both small and large health care organizations deploy firewall capabilities in the following areas: on wide area network (WAN) pipes to the internet and perimeter, across data centers, in building distribution switches, in front of partner WAN/VPN connections, and over wireless networks.

HHS also indicates segmenting networks into security zones is a fundamental method of limiting cyberattacks. These zones can be based on sensitivity of assets within the network (e.g., clinical workstations, general user access, guest networks, medical device networks, building management systems) or standard perimeter segmentations (e.g., DMZ, middleware, application servers, database servers, vendor systems).

7. **Vulnerability management**

The HICP Technical Volumes state effective health care cybersecurity programs use vulnerability management to proactively discover vulnerabilities. According to the HICP Technical Volumes, these processes enable the organization to classify, evaluate, prioritize, remediate, and mitigate the technical vulnerability footprint from the perspective of an attacker. The ability to mitigate vulnerabilities before a hacker discovers them gives the organization a competitive edge and time to address these vulnerabilities in a prioritized fashion.

8. **Incident response**

The HICP Technical Volumes stress while most cybersecurity programs begin by implementing controls designed to prevent cyberattacks against an organization's IT infrastructure and data, it is equally important to invest in and develop capabilities to detect successful attacks and respond quickly to mitigate the effects of these attacks. The HICP Technical Volumes state it is paramount all organizations detect, in near real time, phishing attacks that successfully infiltrate their environment and neutralize their effects before widespread theft of credentials or malware installation occurs.

9. **Medical device security**

The HICP Technical Volumes recommend any device connected directly to a patient for diagnosis or therapy should undergo extensive quality control to ensure it is safe for use. Rigorous stipulations, managed by the FDA, are in place for the development and release of such systems.[5] Device manufacturers should comply with regulations regarding the manufacture of connected medical devices. Organizations that purchase devices and use them for the treatment of patients are the clinical providers. The HICP Publication states that given the highly regulated nature of medical devices and the specialized skills required to modify them, it is ill-advised for organizations that deploy medical devices to make configuration changes without the support of the device manufacturer. Doing so may put the health care organization at risk of voiding warranties, result in legal liabilities, and, at worst, harm the patient. Therefore, the HICP Publication recommends traditional security methods used to secure assets cannot necessarily be deployed in the case of medical devices, and the specific sub-practices regarding effective management of connected medical devices should be followed by health care organizations.

10. **Cybersecurity policies**

The HICP Technical Volumes recommend both small health care organizations and medium to large health care organizations implement cybersecurity policies that describe and the define the following:

- Cybersecurity roles and responsibilities throughout the organization.
- Training that includes common cyberattacks (such as phishing), lost/stolen devices, and methods for reporting suspicious behavior on computers.
- Acceptable use of company data and equipment and acceptable e-mail use.

- How data is to be classified, with usage parameters around those classifications.
- The organization's position on the use of personal devices (i.e., BYOD). If these are permitted, establish expectations for how the devices will be managed.
- Policies for the security of mobile devices and how they are to be used in a remote setting.
- User requirements to report suspicious activities within the organization.
- The requirements for IT security controls in a series of policies or a single long policy. Examples include access control, identity management, configuration management, vulnerability management, and data center management.
- The actions that must be taken to ensure proper identification and protection of all IT assets purchased by the organization.

The HICP Technical Volume for Small Health Care Organizations is available here.

The HICP Technical Volume for Large Health Care Organizations is available here.

The HICP Publication also includes an appendix of cybersecurity resources for health care organizations to access. The appendix includes a glossary of cybersecurity terms, documents used for cybersecurity assessments, links to government agency resources for cybersecurity guidance, and cybersecurity policies and procedures templates that can be adopted by health care organizations. The appendix to the HICP Publication that includes these resources is available here.

More information regarding the HHS-HSSC led task group and a downloadable copy of the entire HICP Publication is available here. If your organization has questions regarding the HICP Publication, the effectiveness of your cybersecurity practices, or other cybersecurity concerns such as HIPAA compliance, please contact a Dinsmore health care attorney for more information.

---

[1] HHS Ransomware Factsheet, available at: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.
[2] See, 45 C.F.R. § 164.308(a)(6).
[3] 21 U.S.C. § 321(h).
[4] The HCIP Technical Volumes reference the EDUCAUSE IAM toolkit for health care organizations looking to implement IAM programs, available here: https://library.educause.edu/resources/2013/5/toolkit-for-developing-an-identity-and-access-management-iam-program/.
[5] The FDA has published separate recommendations for mitigating and managing cybersecurity threats available here: https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm.