Cybersecurity and Hospitals

Four Questions Every Hospital Leader Should Ask in Order to Prepare for and Manage Cybersecurity Risks

American Hospital Association®

This resource was prepared exclusively for American Hospital Association members by Mary Ellen Callahan of Jenner & Block.

Introduction

Cybersecurity has been a hot topic, both within the government and the private sector, for several years. However, the issue recently has taken on even greater prominence. Many organizations, from private media companies to the U.S. Department of Defense, recently disclosed cybersecurity intrusions. Private sector chief executive officers (CEOs) and general counsels have consistently identified cybersecurity threats as one of their top concerns.[1] And in February 2013, President Obama issued an *Executive Order on Improving Critical Infrastructure Cybersecurity* with the goal of improving cybersecurity and reducing cyber threats to the nation's "critical infrastructure sectors," including the Healthcare and Public Health Sector. Despite the attention cybersecurity has received, not everyone knows what cybersecurity is or what it really means for American businesses, particularly for those in the critical infrastructure sectors referenced in the president's executive order.[2]

Hospitals and health care organizations fall into the Healthcare and Public Health Critical Infrastructure Sector under federal law and policy; the executive order uses the same critical infrastructure classifications when identifying the potential impact on the U.S. economy by cybersecurity threats. In other words, the executive order and other government policies collectively identify hospitals' systems and assets as so vital to the U.S. that their impairment would severely threaten public health and safety.[3] As a result, hospitals need to have an awareness of cybersecurity risks, as well as a clear understanding of what their cybersecurity responsibilities are (and how they might intersect with other statutory and regulatory requirements). This paper provides an overview of what cybersecurity is and addresses four questions that hospital leaders should consider when thinking about cybersecurity and how it impacts their organization:

(1) Why should hospitals and hospital leaders care about cybersecurity?

(2) What should hospitals do in response to the 2013 *Executive Order on Cybersecurity?*

(3) How can hospitals best protect their assets and manage cybersecurity risks?

(4) What are the roles of hospital leadership and how can leadership stay informed about cybersecurity threats to the hospital?

This paper is intended to make the cybersecurity issues specifically facing hospitals concrete, identifiable and actionable. It includes an appendix that provides an overview of the 2013 *Executive Order on Cybersecurity* and a glossary of the cybersecurity terms used in general discussions of cybersecurity and in this paper.

I. Why should hospitals and hospital leaders care about cybersecurity?

Cybersecurity vulnerabilities and intrusions pose risks for every hospital and its reputation.

The expanded use of networked technology, Internet-enabled medical devices and electronic databases in administrative, financial and clinical arenas not only brings important benefits for care delivery and organizational efficiency, it also increases exposure to possible cybersecurity threats. Many medical devices and other hospital assets now access the Internet – both in encrypted and unencrypted fashion. Billing systems use electronic transfers, medical devices upload vital statistics in real time to electronic health records, hospitals allow patients and visitors access to hospital WiFi as a courtesy, patients are being provided access to protected health information (PHI) via authentication on the Internet – all of these are important and vital aspects of a modern hospital ecosystem. In addition, email systems are subject to common threats like "spear-phishing."

The number of cyber attacks on American assets has been increasing, particularly in the critical infrastructure sectors such as information technology and communications. Although not as prominently discussed in the media, attacks against the Healthcare and Public Health Sector also are increasing. There are several different types and causes of cybersecurity threats, the names and descriptions of which can be found in the attached glossary. Whatever the cause of the intrusion, the reputational, structural and, potentially, financial impacts for a hospital may be the same. Industrial espionage intrusions against hospitals, for example, have resulted in the theft of information about innovations in medical technology, including system documentation, beta and pilot testing reports, and research notes. Other cyber criminals, whether part of criminal organizations or acting independently, have attempted to penetrate hospitals and health care companies to steal employee data and personally identifiable information and PHI of patients to sell in online black markets. There even exists the threat of cyber terrorism against a hospital, which might include attempts to disable medical devices and other systems needed for the provision of health care.

The Food and Drug Administration (FDA) recently acknowledged this medical device vulnerability when it issued an alert and draft guidance recommending that medical device manufacturers and health care facilities take measures to protect against cybersecurity intrusions that could compromise device performance and patient safety.[4] This could take the form of a direct attack or could be used to multiply the impact of more conventional types of terrorism that result in mass casualties.

Members of the Healthcare and Public Health Sector to some extent already have a unique perspective on data security because of the security requirements of the *Health Insurance Portability and Accountability Act* (HIPAA) and the *Health Information Technology for Economic and Clinical Health Act* (HITECH). These laws not only require hospitals and other health care organization to keep patient PHI secure, but also include data breach notification requirements, which mandate breaches be reported to the Department of Health and Human Services (HHS).

But cybersecurity encompasses much more than what is required by these laws. Notably, cybersecurity intrusions are not limited to data breaches involving PHI. Rather, as noted above, the intent of the intrusion may be to seek information about medical innovations or technologies or may seek to harm patients by remotely disabling or modifying medical devices. Indeed, certain "hacktivists" may seek to disrupt a hospital's network or systems merely for their own personal or political reasons. As a result, the hospital's cybersecurity investigation and incident response plan, discussed in more detail below, should be developed broadly to protect all of a hospital's assets and devices.

In addition to HIPAA and HITECH, hospitals also need to keep in mind additional recommendations and guidance. For example, the Centers for Medicare & Medicaid Services (CMS) has provided a series of information security policies for hospitals[5] and is expected to update those policies to expressly include cybersecurity recommendations. Moreover, publicly traded hospitals should keep in mind the Securities and Exchange Commission's (SEC) October 2011 guidance, which recommends that publicly traded companies disclose to the public both cybersecurity vulnerabilities and intrusions.[6] Prior to the SEC's release of this guidance, even companies without HITECH reporting requirements often would publicly disclose a data *breach* after it had occurred; but companies were less consistent about reporting a cybersecurity *vulnerability* in the absence of a data breach or intrusion. The SEC is revisiting whether the 2011 guidance is sufficient. Of particular note, during the two and a half years following the initial SEC guidance, agency staff contacted several companies that had not disclosed adequately (in staff's opinion) cybersecurity vulnerabilities or intrusions. In light of this fact and the heightened interest in cybersecurity, publicly traded hospitals should consider whether to make any disclosures in their SEC filings concerning cybersecurity vulnerabilities and breaches, in addition to notifying HHS, as appropriate, when there is a data breach involving PHI.

In short, every hospital should care about cybersecurity. As hospitals benefit from networked technology and greater connectivity, they also must ensure that they evaluate and manage new risks. Taking steps to improve the security of each device and the ecosystem, such as documenting the way the devices interact with each other and raising the audit trail capability of the hospital infrastructure, can mitigate the threat to the hospital's overall infrastructure and reduce cybersecurity risks.

II. What should hospitals do in response to the 2013 Executive Order on Cybersecurity?

In response to the president's *Executive Order on Cybersecurity* (and as a corporate best practice), hospitals should develop a cybersecurity investigation and incident response plan or review their existing plans.

Ideally, the plan should be based at least in part on the framework that the National Institute of Standards and Technologies (NIST) is drafting. The executive order instructs the director of the National Institute of Standards and Technology (NIST) of the Department of Commerce to finalize by Feb. 12, 2014, a "Cybersecurity Framework" to help owners and operators of critical infrastructure identify, assess and manage the risk of cyber threats.

The framework will include general standards and considerations for all entities establishing cybersecurity plans. As a result, the standards and considerations in the framework will need to be fine-tuned for hospital-specific requirements, such as incorporating accountability for medical devices. NIST has been conducting public outreach on a draft Cybersecurity Framework, including town halls and working sessions.

When completed early next year, the Cybersecurity Framework will be voluntary for critical infrastructure-sector organizations such as hospitals; for federal departments and agencies, in contrast, it will be required. Importantly, although the framework is designated as "voluntary" for private-sector owners and operators of critical infrastructure, hospitals should anticipate that the framework will likely be considered a *de facto* baseline for general cybersecurity compliance. Significant non-conformity with the framework, therefore, may increase the likelihood of litigation and enforcement risk.

The executive order also directs the creation of a "Voluntary Critical Infrastructure Cybersecurity Program," which will provide incentives for private-sector organizations to adopt the framework. Owners and operators of critical infrastructure, such as hospitals who participate in the Voluntary Critical Infrastructure Cybersecurity Program, will be responsible for identifying, assessing and managing their cyber risks in accordance with the standards set out in the Cybersecurity Framework under development. Because the framework will provide participants with flexible baseline standards for addressing cyber risks, rather than a comprehensive list of requirements, hospitals participating in the program will need to determine how best to implement the standards through concrete internal rules and protocols tailored for their specific organization.

Hospitals also should consider engaging in regional or national information-sharing organizations such as the Healthcare and Public Health Sector Coordinating Council (HPH SCC),[7] the National Health Information Sharing and Analysis Center (NH-ISAC)[8] and the Health Information Trust Alliance (HITRUST).[9] As appropriate, hospitals also can consider having a representative regularly attend local and state emergency planning committees to provide awareness and continuing education of the evolving threats. Hospitals' participation is consistent with the executive order's emphasis on the importance of information sharing.

The focus of the executive order largely is on intra-government activities, such as how federal government departments and agencies can improve internal cybersecurity infrastructure and sharing classified and unclassified information with each other, and with organizations in critical infrastructure sectors. However, the executive order and the accompanying *Presidential Policy Directive 21* also designate specific federal agencies, referred to as "Sector-Specific Agencies," to coordinate cybersecurity efforts within each critical infrastructure sector and to share information about cybersecurity threats with the owners and operators within the sectors. HHS is the Sector-Specific Agency directed to work with and provide guidance to hospitals and health care organizations, as part of the Healthcare and Public Health Sector (see Appendix for brief overview of the executive order and the related *Presidential Policy Directive 21*).

Top Six Actions to Manage Hospital Cybersecurity Risks

1. Establish procedures and a core cybersecurity team to identify and mitigate risks, including board involvement as appropriate.

2. Develop a cybersecurity investigation and incident response plan that is mindful of the Cybersecurity Framework being drafted by the National Institute of Standards and Technology.

3. Investigate the medical devices used by the hospital in accordance with the June 2013 FDA guidance to ensure that the devices include intrusion detection and prevention assistance and are not currently infected with malware.

4. Review, test, evaluate and modify, as appropriate, the hospital's incident response plans and data breach plans to ensure that the plans remain as current as possible in the changing cyber threat environment.

5. Consider engaging in regional or national information-sharing organizations to learn more about the cybersecurity risks faced by hospitals.

6. Review the hospital's insurance coverage to determine whether the current coverage is adequate and appropriate given cybersecurity risks.

III. How can hospitals best protect their assets and manage cybersecurity risks?

Cybersecurity is not an absolute, immobile standard – it is an evolving one that changes with the newest threats and vulnerabilities.

A hospital's cybersecurity plan, therefore, must be just as flexible and resilient in the face of multi-pronged cybersecurity threats. The inter-connectivity of hospital assets and services, and the information security infrastructure, have created a constantly evolving network with ever-changing threats and vulnerabilities to discover, evaluate and manage. A resourceful and resilient hospital will prepare for these risks as it does the other risks it faces – with planning, testing and response.

One key to managing cybersecurity risks is to make cybersecurity part of the hospital's overall governance, risk management and business continuity framework. For example, a hospital may want to integrate the cybersecurity investigation and incident response plan into its overall all-hazards emergency operations plan and ensure that staff are informed about cybersecurity and their roles in mitigating risks. Given already-existing robust statutory and industry standards, cybersecurity should be viewed not as a novel issue but as an additional hazard that should be taken into account in the hospital's inclusive hazards vulnerability analysis.

Specifically, hospitals should:

- Create a hospital-wide cybersecurity investigation and incident response plan. This will be similar to the HITECH plan you likely already have in place for any data breach involving patients' PHI. In fact, you can incorporate many of the elements from your data breach plan into your cybersecurity plan. In addition to those elements, however, the cybersecurity investigation and incident response plan should address other elements, including system-wide impacts, responding to spear-phishing or penetration attacks, auditing log files and other records, and identifying all exfiltrated data and inappropriate access, regardless of whether the breach involves patients' PHI.

- Evaluate and document the medical devices that use WiFi/Internet services to transmit PHI and ensure they are secure. As the FDA recommended in June 2013, medical devices should be investigated to determine whether they have intrusion detection and prevention assistance on them or whether malware already exists on hospital assets including computers, tablets and databases. In addition, hospitals should consider how best to ensure critical functionality of medical devices in the event of a cyber attack and how to restrict unauthorized access to the hospital's network through networked medical devices. In addition, laboratory systems and networks, hospital and treatment center information systems, department–specific information systems, patient databases, hardware components and software should all be part of the hospital's cybersecurity investigation and incident response plan.

- Periodically test the plan response and processes both theoretically and as a table-top exercise. The hospital also should adopt a proactive approach to identifying and investigating incidents, even when they appear minor. Although an incident may be determined not to be a cybersecurity incident, the more training and familiarity hospital staff have with the processes, the more smoothly the response will go, if and when there is a cybersecurity intrusion.
- Develop an information sharing process (after consultation with cybersecurity or antitrust counsel) for sharing cybersecurity incidents with the regional or national information-sharing organizations with whom your hospital participates.

With respect to the Cybersecurity Framework under which hospitals and other critical infrastructure sectors will soon be operating, hospitals should work through their associations (including the AHA or state hospital associations) to design a strategy to collaborate with HHS to ensure any sector-specific rules both cover each threat or vulnerability that needs to be covered and are limited only to issues that are not already addressed by HIPAA and HITECH. Sector-Specific Agencies, including HHS, are required to coordinate with the Sector Coordinating Councils (such as the Healthcare and Public Health Sector Coordinating Council) to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments. Hospitals, among the other sector participants, may be in a unique position to describe the threats and vulnerabilities that they face every day with respect to cybersecurity. The required coordination provides a perfect opportunity for hospitals to ensure that HHS addresses all the known threats and narrowly tailors any additional recommendations or requirements on hospitals to those that are not otherwise covered by law.

IV. What are the roles of hospital leadership and how can leadership stay informed about cybersecurity threats to the hospital?

Another benefit of incorporating cybersecurity risk into the hospital's overall governance, risk management and business continuity framework is that hospital leadership will stay informed about cybersecurity threats to the hospital and its assets.

Much of the cybersecurity plan will fit into the leadership and management rubric already in place at the hospital. For example, the hospital board should be briefed periodically on the cybersecurity threats and responses, with cybersecurity assigned to the relevant committee of the board for more detailed oversight and governance. The cybersecurity investigation and incident response plan should be shared with the board committee, and periodic review should be scheduled. If there is a cybersecurity intrusion, particularly one of significant magnitude, the board or oversight committee should be briefed on any "lessons learned," as well as proposed plan modifications, with appropriate follow up. The board's audit committee also should have insight and oversight into cybersecurity vulnerabilities and potential exposures (such as insurance coverage).

The hospital's CEO should have regularly scheduled meetings with the chief information officer (CIO) and/or other members of the hospital's cybersecurity team. This team may include the CIO, who generally has responsibility for the information technology and computer systems that support enterprise goals, including information security; the chief technology officer, who generally oversees the development and integration of new technologies, a chief information security officer, who often reports to the CIO or chief operating officer and whose responsibilities include developing a strategy and approach to protect hospital electronic assets, including medical devices;[10] a chief security officer with responsibilities for physical security at the hospital; and leaders of the clinical team. These meetings may cover development of and compliance with the cybersecurity investigation and incident response plan, the results of any table-top exercises performed by the hospital staff, and the evolving nature of the threats, vulnerabilities and risks that the hospital faces.

In addition to the core cybersecurity team, the hospital's legal department, human resources department and training staff should have an active role in developing and implementing the cybersecurity investigation and incident response plan.

While the cybersecurity investigation and incident response plan is being developed, the team also should review information security policies and procedures generally as part of the all-hazards emergency operations plan. The hospital's general counsel or insurance counsel also should review its insurance coverage to plan and evaluate its cybersecurity risk profile, to determine what insurance coverage is available and appropriate. There are a wide range of coverage options available for cybersecurity vulnerabilities and incidents, including new cyber risk policy forms.

Endnotes

[1] *See, e.g.,* June 17 interview with Honeywell CEO David Cote, "[cybersecurity] is the one that scares me the most"; in the 2012 Consero survey of private sector general counsels, 28% of companies had experienced a cybersecurity breach over the last 12 months, and 30% did not believe they were prepared for a cybersecurity incident. *http://consero.com/2012-general-counsel-data-survey/*

[2] "Critical Infrastructure" was first codified in the U.S. in 1996, and then added in the USA Patriot Act in 2011; the 16 sectors are listed at: *http://www.dhs.gov/critical-infrastructure-sectors*

[3] The Executive Order defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

[4] *FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks*, (June 13, 2013) available at: *http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm*. In conjunction with the FDA's alert, the U.S. Department of Homeland Security issued a separate alert warning that an estimated 300 medical devices from 40 vendors could be vulnerable to hacking and that "the vulnerability could be exploited to potentially change critical settings and/or modify device firmware."

[5] *https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS_Policy-.pdf*.

[6] *http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.*

[7] *http://www.dhs.gov/xlibrary/assets/nppd/nppd-ip-healthcare-and-public-health-snapshot-2011.pdf*

[8] *http://www.nhisac.org/nh-isac/*

[9] *http://www.hitrustalliance.net/*

[10] The incorporation of a chief information security officer (CISO) into hospital leadership is a recent trend among larger hospitals that demonstrates the need for integrating specialists addressing information security and cybersecurity. If the hospital has a CISO, he/she will be essential to the cybersecurity team.

Appendix

February 12, 2013 Executive Order on Cyber Security Summary and Presidential Policy Directive 21

On Feb. 12, 2013, President Barack Obama issued an executive order titled, "Improving Critical Infrastructure Cybersecurity." Although the executive order lacks the force of law (such as that of a statute enacted by Congress or a formal regulation issued by a government agency), it makes substantial advancements to the nation's cybersecurity monitoring and response systems.

In general, the executive order gives four directives to federal agencies to protect the nation's "critical infrastructure" from cyber threats: 1) facilitate increased and improved sharing of cybersecurity information among federal agencies and the owners and operators of critical infrastructure (which includes hospitals and other health care organizations); 2) establish a framework to reduce the risk of cyber threats; 3) identify the nation's critical infrastructure most at risk for cyber attacks; and 4) allow Sector-Specific Agencies to establish voluntary Critical Infrastructure Cybersecurity Programs. The executive order defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

1) Information Sharing

To improve information sharing among government agencies and the owners and operators of critical infrastructure, the executive order directs the Attorney General, Secretary of the Department of Homeland Security (DHS) and the Director of National Intelligence to establish a process for declassifying information about cyber threats and disseminating it quickly to the appropriate stakeholders, including hospitals.

On the same day the president issued the executive order, he also signed *Presidential Policy Directive 21, Critical Infrastructure Security and Resilience*. The directive aims to improve information sharing and responses regarding cybersecurity threats. The directive defines 16

Presidential Policy Directive-21 identifies 16 critical infrastructure sectors:

- **Chemical**
- **Commercial Facilities**
- **Communications**
- **Critical Manufacturing**
- **Dams**
- **Defense Industrial Base**
- **Emergency Services**
- **Energy**
- **Financial Services**
- **Food and Agriculture**
- **Government Facilities**
- **Healthcare and Public Health**
- **Information Technology**
- **Nuclear Reactors, Materials and Waste**
- **Transportation Systems**
- **Water and Wastewater Systems**

"Critical Infrastructure Sectors" and assigns each sector a "Sector-Specific Agency." For health care and public health, the Department of Health and Human Services (HHS) is the Sector-Specific Agency.

The information-sharing entities created by the directive are examples of Information Security and Analysis Centers (ISACs). These entities, which already exist at various levels of government and among private industries, are created by a group of members, such as a group of corporations with similar data and cybersecurity needs and challenges, to facilitate collaboration in responding to cybersecurity threats.

2) The Cybersecurity Framework

The executive order also instructs the director of the National Institute of Standards and Technology (NIST) of the Department of Commerce to create a "Cybersecurity Framework" to help owners and operators of critical infrastructure identify, assess and manage the risk of cyber threats. The framework will consist of various policies and procedures for addressing cyber risks based on voluntary consensus standards and industry practices. NIST has been conducting public outreach on a draft Cybersecurity Framework, including town halls and working sessions. NIST is required by the executive order to finalize the framework by Feb. 12, 2014.

3) Identify the Most Critical Infrastructure

The executive order also directs DHS to identify at-risk critical infrastructure "where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security or national security." DHS will then notify the owners and operators of that infrastructure confidentially and will provide them with relevant information on cybersecurity risks.

4) Voluntary Critical Infrastructure Cybersecurity Program

Sector-Specific Agencies, including HHS, are required to coordinate with the Sector Coordinating Councils (such as the Healthcare and Public Health Sector Coordinating Council) to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments. Participation in the program will be voluntary; the executive order directs the secretaries of DHS, Treasury and Commerce (but not HHS) to determine what incentives will be provided to participants within the critical infrastructure sectors.

Expectations of Owners and Operators of Critical Infrastructure under the Executive Order

The executive order directs the creation of a Cybersecurity Framework, in part, to provide owners and operators of critical infrastructure with guidance on how to identify and address cyber risks. Although the framework will not be binding on private-sector companies, it will aim to reflect industry standards and best practices as much as possible. The executive order also directs the creation of a Voluntary Critical Infrastructure Cybersecurity Program, which will provide incentives for private-sector organizations to adopt the framework. Owners and operators of critical infrastructure such as hospitals that participate in the Voluntary Critical Infrastructure Cybersecurity Program will be responsible for identifying, assessing and managing their cyber risks in accordance with the standards set out in the Cybersecurity Framework. Because the framework will provide participants with flexible baseline standards for addressing cyber risks, rather than a comprehensive list of requirements, hospitals participating in the program will need to determine how to implement the standards through concrete internal rules and protocols.

Glossary of Key Cybersecurity Terms

What is "cybersecurity," or a "cyber attack"?

To understand the scope and effects of the executive order, one must be familiar with several key cybersecurity terms:

- **Cybersecurity:** A broad term that is frequently used but infrequently defined; in general, "cybersecurity" refers to a set of standards and practices employed to prevent unwanted intrusions into computer systems, sometimes referred to as "cyber attacks." The executive order does not define these terms, but uses them repeatedly. Cybersecurity can be seen as the "process of preventing unauthorized modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient" (FDA definition, June 2013 Alert).
- **Cyber Attack (or "cybersecurity threat"):** Another common term that is often left undefined in the cybersecurity literature; the most useful way to understand a cyber attack is to consider the three general forms of cyber attacks:
  - **Advanced, Persistent Threats:** A cyber attack perpetrated or facilitated by a foreign government (or sometimes other sophisticated organizations) against the government or industry of another nation, typically for geopolitical or strategic reasons. Such attacks are referred to as "advanced" and "persistent" because the large resources and sophistication of the attackers allow the attacks to take a variety of forms over an extended period of time.
  - **Organized Cyber Crime:** A cyber attack perpetrated by a criminal organization in order to defraud or steal from victims. Such attacks often take the form of large-scale efforts to steal financial or other sensitive information from individuals or from large organizations such as banks and retailers.
  - **Individual Interests:** A cyber attack perpetrated by small groups or individuals, such as "hacktivists" or a disgruntled former employee.

Other Key Cybersecurity Terms

- **Critical Infrastructure:** Defined in the executive order as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Directive 21 identifies "Healthcare and Public Health" as a Critical Infrastructure Sector.

- **Critical Infrastructure Partnership Advisory Council (CIPAC):** An entity of DHS responsible for facilitating coordination between federal, state, local and tribal governments, and the private sector, to protect critical infrastructure. Among the membership of CIPAC are the members of each of the 16 critical infrastructure sectors, including the Healthcare and Public Health Sector Coordinating Council. The executive order instructs the director of DHS to consider the advice of the CIPAC in coordinating public-private partnerships to manage cybersecurity risk. CIPAC will have a primary coordinating role in the Voluntary Critical Infrastructure Cybersecurity Program.

- **Cybersecurity Investigation and Incident Response Plan:** Such a plan will identify steps to investigate, ameliorate, remedy and respond to cybersecurity intrusions. This plan will incorporate hospitals' data breach plan under the *Health Information Technology for Economic and Clinical Health Act* (HITECH), but will need to address other elements such as system-wide impacts, spear-phishing or penetration, auditing log files and other records, and identifying exfiltration and inappropriate access, even if it is not related to protected health information (PHI).

- **Cybersecurity Intrusion (also known as Cybersecurity Incident):** An unauthorized access to computer systems, databases or electronic files. Intrusions can be accomplished by spear-phishing.

- **Cybersecurity Vulnerability (also known as Cybersecurity Risks):** Weakness or flaws in information security systems and system architecture.

- **Distributed Denial of Service (DDoS) Attack:** A type of cyber attack in which the attacker overwhelms the resources of the targeted computer system in order to prevent others from using the system normally (for example, by flooding a website with excessive visits until it crashes and cannot accept new visitors).

- **Exfiltration:** Sometimes referred to as "extrusion," the unauthorized removal of data from a computer system.

- **Exploitation:** The use of a software program or other piece of computer code to take advantage of a vulnerability in a computer system, typically in order to disrupt or prevent normal use of that system. The software program or code used in such an attack is often referred to as an "exploit."

- **Healthcare and Public Health Sector Coordinating Council (HPH SCC):** Organization established by HHS that comprises six sub-councils representing private sector industries and interest areas within the sector. The six sub-councils represent many healthcare sectors including direct health care, health information and medical technology, health plans and payers, mass fatality management, medical materials, and pharmaceuticals, laboratories and blood banks. The SCC is a self-governing body that provides a forum for the private sector to discuss infrastructure protection issues and communicate with government. The SCC, along with the Government Coordinating Council (GCC), which includes representatives from all levels of government, has created a variety of work groups including work groups related to information sharing and cybersecurity.

- **Honey Pot:** A "trap" used to detect and thwart cyber attacks, typically in the form of a computer system or website that appears to be part of a particular network but which is actually isolated and monitored. Certain sophisticated types of honey pots can be used to gain information about the motives and tactics of perpetrators of cyber attacks.

- **Insider Threat:** An attack on a computer system perpetrated by someone on the "inside" of an organization—often an employee or former employee, or independent contractor—who may possess confidential information about the organization's data security and management systems which facilitates the exploitation of proprietary systems.

- **Information Security and Analysis Centers (ISACs):** Associations of various member entities, including government agencies and private corporations, with similar or related cybersecurity needs and challenges, formed to facilitate collaboration in identifying and responding to cybersecurity threats. ISACs, such as the National Health ISAC (NH-ISAC), typically serve as public-private partnerships between federal, state and local governments and a particular private industry sector. The partnerships identified in Directive 21 between the Critical Infrastructure Sectors and their corresponding Sector-Specific Agencies are examples of ISACs.

- **Malware:** A general term for a malicious software program (including a computer virus, a worm, spyware, adware, etc.) used to disrupt the normal operation of a computer system or to exfilrate information from that system.

- **Phishing:** A type of cyber attack that seeks to install malware and gain access to corporate computer systems by posing as a familiar or otherwise trustworthy website or entity:

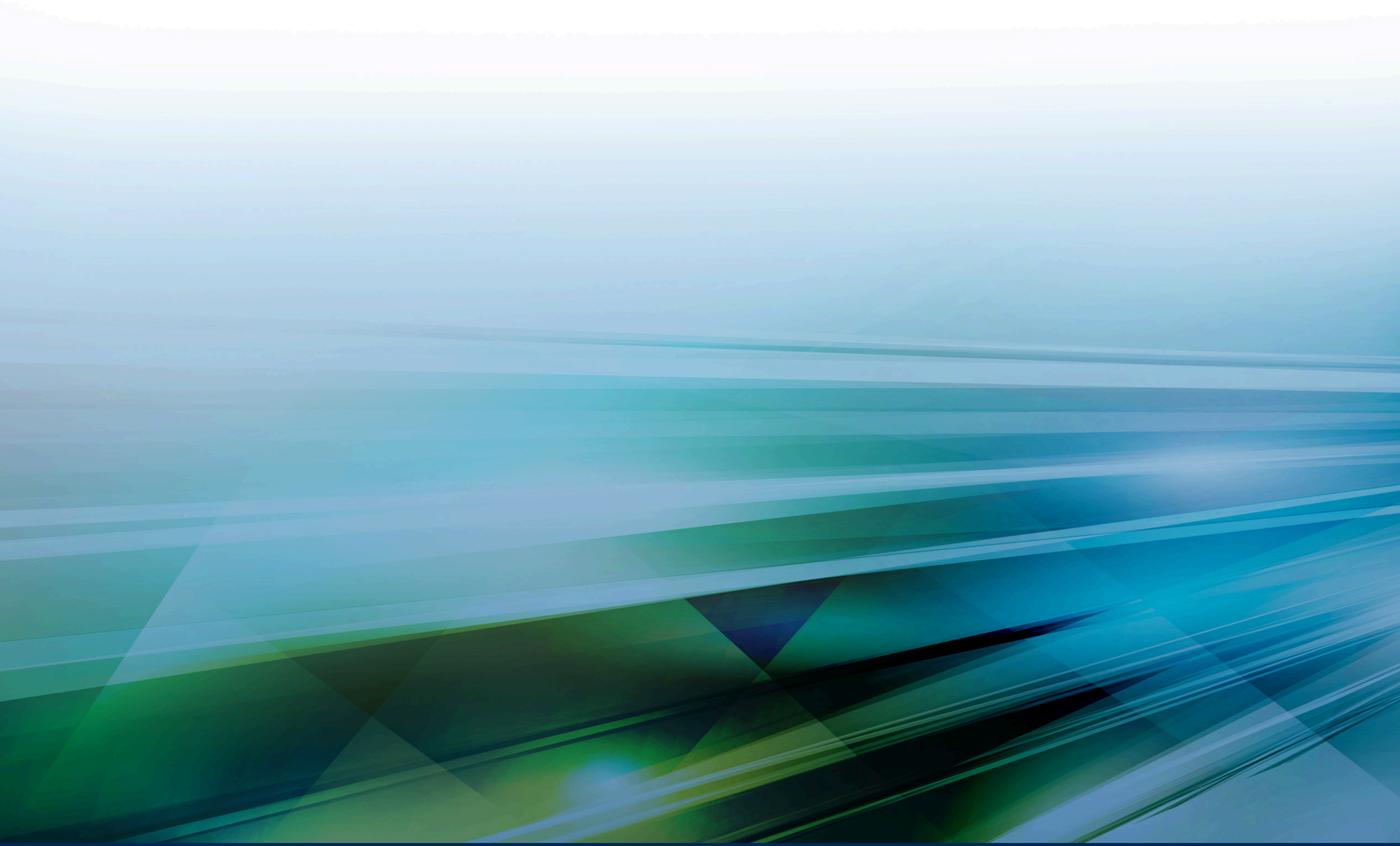
  - **Spear-Phishing:** A type of phishing that is targeted at a specific individual. Perpetrators may first gather personal information about the target, such as what websites the individual frequents or which bank he or she uses, in order to make the deception more believable and increase the chance of success.

  - **Whale-Phishing:** A spear-phishing attack directed at a high-profile individual, such as a senior corporate executive.

  - **Smishing:** A combination of SMS texting and phishing

  - **Vishing:** Voice and phishing

- **United States Computer Emergency Readiness Team (US-CERT or CERT):** An entity within DHS responsible for coordinating information sharing and responses to cyber threats. CERT regularly issues alerts and bulletins regarding current cyber threats and provides recommendations for addressing those threats.



Chicago Office:
155 N. Wacker Drive
Chicago, Illinois 60606
312.422.3000

Washington Office:
325 7th Street, N.W.
Washington, DC 20004
202.638.1100

www.aha.org/cybersecurity

American Hospital
Association®

9/2013