In the wake of the recent WannaCry Ransomware cyber attack that is believed to have started at Britain’s National Health Services (NHS) before quickly spreading to more than 200 countries, the U.S. government is urging the healthcare industry to take further precautions regarding cybersecurity and is deploying tools to assist organizations in responding to immediate threats and implement stronger security measures.

**WannaCry Ransomware**

On May 12, 2017, the WannaCry Ransomware worm infected the information systems of 47 NHS organizations and caused widespread disruption of patient care and operations at NHS hospitals and facilities, including the interruption of telephone communications and the instantaneous loss of access to patient records, etc. As WannaCry continued to spread rapidly across the globe, NHS, the U.S. government and experts from the private sector collaborated to warn the public at large and attempt to develop a patch.

The WannaCry attack and the rise of sophisticated ransomware attacks paralyzing operations and patient-critical devices underscore the vulnerability of the healthcare system in the U.S. and abroad. Today, digital connectivity in the healthcare industry is ubiquitous and paramount to the safe and efficient delivery of patient care. But the risks are real and multi-faceted—fraud, identity theft, data privacy breaches, ransomware, supply chain disruptions, research and development theft, stock manipulations, etc. Such risks add exponentially to the already complex (and at times conflicting) state, federal, and payor-driven framework of rules and regulations inherent to the U.S. healthcare industry.

At a time when all healthcare organizations should take enhanced measures to secure their systems and information technology (IT) infrastructure, significant differences exist among the various industry stakeholders in terms of resources and awareness. The U.S. healthcare system is a matrix of diverse providers and suppliers with very disparate IT resources serving a mosaic of patient populations. Yet, all constituents, whether a large health system, a small/rural hospital, a private or public payor, a medical device or software manufacturer, must recognize that healthcare cybersecurity is a key public health concern that requires focus and attention at the leadership level. The U.S. government is trying to bridge some of these disparities and heighten awareness at the macro and industry specific level.

**The National Cybersecurity and Communications Integration Center**

Within the Department of Homeland Security (DHS), the National Cybersecurity and Communications Integration Center (NCCIC) is tasked with analyzing cybersecurity and communications information, sharing timely and actionable information, and coordinating response, mitigation, and recovery efforts in the event of a cyber threat or attack. It serves as a central location where government agencies, the private sector, and international entities involved in cybersecurity and communications protection coordinate and synchronize their efforts. The NCCIC’s mission is “to operate at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities, applying unique analytic perspectives, ensuring shared situational awareness, and orchestrating synchronized response efforts while protecting the constitutional and privacy rights of Americans in both the cybersecurity and communications domains.” In the healthcare industry, the four branches of the NCCIC (see Figure 1 below), which are (1) the NCCIC Operations & Integration (NO&I), (2) the United States Computer Emergency Readiness Team (US-CERT), (3) ICS-CERT, and (4) the National Coordinating Center for Communications (NCC), work closely with the Department of Health and Human Services (HHS), the Office of Civil Rights (OCR)—which has jurisdiction over HIPAA breaches, and the Health Care Industry Cybersecurity (HCIC) Task Force.

**Healthcare Cybersecurity**

Although the vast majority of healthcare providers know that they have certain obligations under the HIPAA laws to protect the privacy and security of patient data, research shows that many underestimate the meaning, planning, and training required to fulfill such obligations. In addition, most constituents underestimate the imminence and scope of cyber threats such as ransomware. The OCR and the U.S. Government Accountability Office’s (GAO) data clearly shows a sharp increase in, and acceleration of, the number of data breaches affecting more than 500 healthcare records since 2010. In 2010, only 10 major breaches were reported. This number had grown to 56 in 2015 and, as of the date of publication of this article, the OCR has already recorded at least 132 major breaches for the first five-and-a-half months of 2017. U.S. government agencies work assiduously to track cyber incidents and warn the public. In February 2017, just a few months prior to the WannaCry attack, the OCR highlighted this alarming trend in its guidance publication, Reporting and Monitoring Cyber Threats, and urged healthcare actors to take proactive steps such as reporting all suspicious activities and indicators to the US-CERT portal.

Although non-binding, healthcare entities and

---

**Figure 1, Office of Cybersecurity & Communications Organizational Structure**

---
business associates should review the OCR’s recommendations and sign up for email alerts about rising threats.

U.S. government agencies also protect the public by deploying and sharing their expert knowledge during and after cyber emergencies. For example, in response to the WannaCry attack, the HHS issued warnings to healthcare organizations and suggested some basic first steps to protect against ransomware attacks:

- Only open up emails from people you know and that you are expecting. The attacker can impersonate the sender, or the computer belonging to someone you know may be infected without his or her knowledge.
- Do not click on links in emails if you were not expecting them. For example, the attacker could camouflage a malicious link to make it look as if it is from your bank.
- Keep your computer and antivirus software up to date—this adds another layer of defense that could stop the malware.

In addition, HHS recommends the following steps to victims of ransomware: (1) contact the FBI Field Office Cyber Task Force immediately to report the ransomware event and request assistance. The FBI works with state and local law enforcement and other federal and international partners to pursue cyber criminals globally; (2) report cyber incidents to US-CERT and the FBI’s Internet Crime Complaint Center; and (3) share healthcare-specific indicators with HHS’ Healthcare Cybersecurity and Communications Integration Center (HCCIC), aka the Fusion Center (HHS’ own version of the NCCIC), a central location for information-sharing across HHS and federal government partners to provide data and tools to aid in fusion efforts to support threat analysis organizations (ISAOs), including appropriate safeguards are in place for such devices. Medical devices’ failure due to cyberattack can be triggered by the introduction of malware into the medical equipment or by unauthorized access to configuration settings in devices and hospital networks.

Cybersecurity Frameworks
Healthcare providers seeking systems’ interoperability, the implementation of connected medical devices, or the enhanced utilization of EHRs should consider cybersecurity frameworks (CSFs) in the mix of the resources they deploy and utilize. Two of the most common CSFs are the National Institute of Standards and Technology (NIST) CSF and Health Information Technology Trust Alliance (HITRUST) CSF. The NIST CSF, Framework for Improving Critical Infrastructure Cybersecurity, was first published in February 2014 and has recently been updated. Unlike the HITRUST CSF, it is not specific to the healthcare industry. The HITRUST CSF includes federal and state regulations as well as globally recognized industry standards, regulations, and business requirements in an effort to normalize security requirements and provide clarity and consistency to healthcare organizations seeking to strengthen the privacy of patients’ records.

Medical Devices Cybersecurity
Medical device manufacturers and healthcare facilities utilizing medical devices should refer to the U.S. Food and Drug Administration’s (FDA) own recommendations to assure that appropriate safeguards are in place for such devices. Medical devices’ failure due to cyberattack can be triggered by the introduction of malware into the medical equipment or by unauthorized access to configuration settings in devices and hospital networks.

Healthcare Industry Cybersecurity Task Force
Established by Congress in 2015, the Healthcare Industry Cybersecurity (HCIC) Task Force brings together healthcare and IT industry representatives to analyze the wide range of cyber threats that affect the healthcare industry and provide pragmatic imperatives and recommendations to strengthen the security of the system. The Task Force recently published its 2017 landmark "Report on Improving Cybersecurity in the Health Care Industry," in which it describes and addresses a non-exhaustive list of 151 potential risks to the confidentiality, availability, and integrity of patient data, as well as to patient safety. Across providers, pharmacies, health plans and payors, health information and medical technology providers, laboratories, patient service centers, medical devices and equipment manufacturers, and pharmaceutical companies, over half of the risks identified (55%) pertain to the loss of PHI. Some of the key risks highlighted in the report include the following:

- Failure to provide timely security software updates and patches to medical devices and networks and to address-related vulnerabilities in older medical device models (legacy devices).
- Malware, which alters data on a diagnostic device.
- Device reprogramming, which alters device function (by unauthorized users, malware, etc.).
- Denial of service attacks, which make a device unavailable.
- Exfiltration of patient data or PHI from the network.
- Unauthorized access to the healthcare network, which allows access to other devices.
- Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel).
- Security vulnerabilities in off-the-shelf software due to poorly designed software security features.
- Improper disposal of patient data or information, including test results or health records.
- Misconfigured networks or poor network security practices.
- Open, unused communication ports on a device which allow for unauthorized, remote firmware downloads.

In light of these risks, the Task Force developed six overarching imperatives and cascading recommendations: (1) define and streamline leadership, governance, and expectations for healthcare industry cybersecurity; (2) increase the security and resiliency of medical devices and health IT; (3) develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities; (4) increase healthcare industry readiness through improved cybersecurity awareness and education; (5) identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure; and (6) improve information-sharing of industry threats, weaknesses, and mitigations. The Task Force recommendations are not yet implemented, nor adopted and funded. Healthcare organizations should, however, leverage the report’s findings in formulating their own priorities and in mitigating risks and HIPAA breaches.

As seen with the recent WannaCry cyber attack, there is still tremendous room for improvement in the realm of healthcare cybersecurity, but government and private
A Cybersecurity Update and Resource Guide for Healthcare Organizations (Continued from page 7)

sector constituents alike are beginning to pay close attention. Leveraging the resources and data made available by the various U.S. government agencies may assist healthcare organizations in reinforcing their own cybersecurity and addressing emerging cyber threats. However, such efforts should not be at the cost of intrinsic HIPAA compliance. Covered entities and business associates should still conduct a thorough review of their HIPAA policies and procedures, confirm that those policies and procedures have actually been implemented, and assess their effectiveness on a continuing basis.

Following and documenting these steps, and in particular conducting an independent HIPAA audit followed by corrective actions, can help organizations demonstrate their good faith and due diligence to the OCR if a breach occurs.

Isabelle Bibet-Kalinyak, Richard C. Cooper, James J. Giszczak, and Rick L. Hindmand are business attorneys with the law firm of McDonald Hopkins LLC (www.McDonaldHopkins.com). James is the Chair of the Litigation Department and Co-Chair of the Data Privacy and Cybersecurity Practice Group; Richard is the manager of the firm’s National Healthcare Practice Group and the Co-Chair of its Healthcare Restructuring Practice Group; Rick’s practice focuses on healthcare regulatory, data privacy, cybersecurity, corporate, and transactional matters; and Isabelle’s practice focuses on healthcare regulatory and transactional matters, as well as business immigration, primarily in healthcare settings.

3. Available at https://www.us-cert.gov/cas/alerts/TA17-132A
4. The sizeable investments in electronic health records (EHRs) systems spurred by the Health Information for Economic and Clinical Health Act and the Meaningful Use incentives have transformed the industry's connectivity and bolstered data use in devices and research.
5. Available at https://www.us-cert.gov/nccic
7. Available at https://www.us-cert.gov/cas/alerts/TA17-132A
12. Available at www.fbi.gov/contact-us/field/offices
13. Available at https://www.us-cert.gov/cas
15. Email HCCIC at HCCIC_RM@hhs.gov
18. As defined in the HIPAA law, 45 C.F.R. Section 160.103.
22. For additional information about HIPAA audits, see Rick L. Hindmand et al., Phase 2 HIPAA Audits Are Coming (March, 28, 2016), available at https://mcdonaldhopkins.com/insights/alerts/2016/03/28/Phase-2-hipaa-audits-are-coming