



Medicare Lacks Consistent Oversight of Cybersecurity for Networked Medical Devices in Hospitals

Key Results

Medicare accreditation organizations (AOs), which derive their requirements from the Conditions of Participation and oversee most Medicare-participating hospitals, rarely use their discretion to examine the cybersecurity of networked devices during their hospital surveys. As a result, Medicare lacks consistent oversight of networked device cybersecurity in hospitals.

Why OIG Did This Review

Without proper cybersecurity controls, hospitals' networked medical devices (i.e., devices designed to connect to the internet, hospital networks, and other medical devices) can be compromised, which can lead to patient harm. The Centers for Medicare & Medicaid's (CMS's) survey protocol for overseeing hospitals is silent with respect to the cybersecurity of these devices. This evaluation sheds new light on the extent to which Medicare AOs use their discretion to address cybersecurity of networked devices during hospital surveys. As hospitals continue to face cyberattacks that risk patient harm, it is important to know whether and how AOs hold hospitals accountable for cybersecurity of their devices.

How OIG Did This Review

We conducted structured telephone interviews with leadership at the four AOs and sent written questions to CMS. We asked the AOs about the extent to which their survey standards required hospitals to have a cybersecurity plan for networked devices, as well as other ways in which their surveys might cover cybersecurity for networked devices. We also reviewed AO documentation of relevant survey standards and procedures.

What OIG Found

CMS's survey protocol does not include requirements for networked device cybersecurity, and the AOs do not use their discretion to require hospitals to have such cybersecurity plans. However, AOs sometimes review limited aspects of device cybersecurity. For example, two AOs have equipment-maintenance requirements that may yield limited insight into device cybersecurity. If hospitals identify networked device cybersecurity as part of their emergency-preparedness risk assessments, AOs will review the mitigation plans. AOs told us that in practice, however, hospitals did not identify device cybersecurity in these risk assessments very often. Assessing hospital safeguards for the privacy of medical records may prompt AOs to examine networked devices. Finally, CMS and the AOs do not plan to update their survey requirements to address networked devices or general cybersecurity.

What OIG Recommends

We recommend that CMS identify and implement an appropriate way to address cybersecurity of networked medical devices in its quality oversight of hospitals in consultation with HHS partners and others. CMS stated that it concurred with considering additional ways to appropriately highlight the importance of cybersecurity of networked medical devices for providers in consultation with its HHS partners that have specific oversight authority regarding cybersecurity. We look forward to CMS's sharing, in its Final Management Decision, its plan for addressing cybersecurity of networked medical devices under its own authority for quality oversight of hospitals.

BACKGROUND

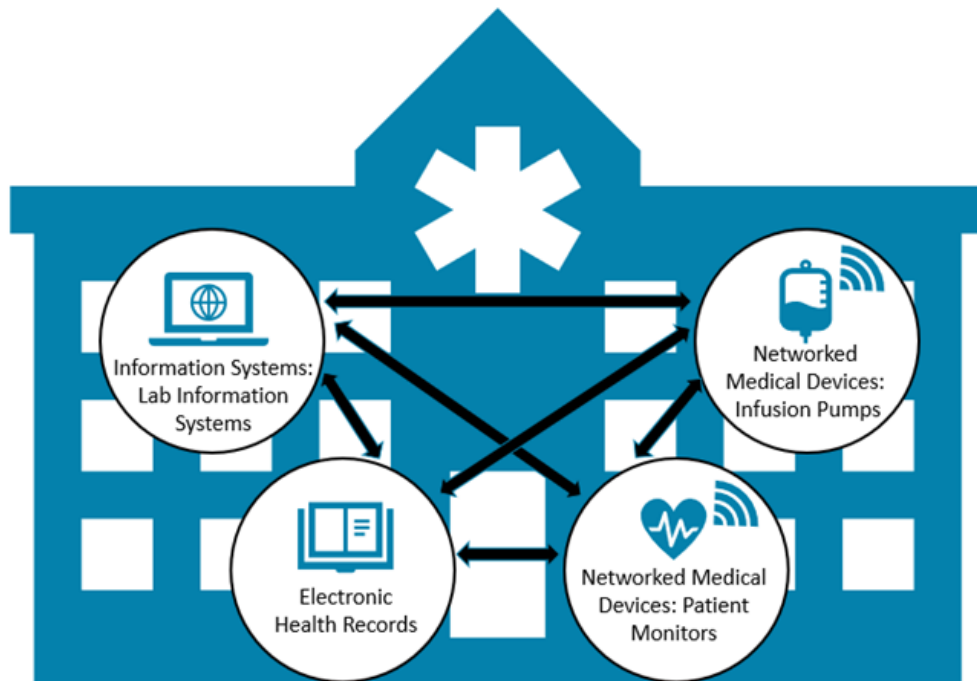
Networked medical devices (hereinafter referred to as networked devices) are devices that are designed to connect to the internet, hospital networks, and other medical devices to provide features that improve health care and increase the ability of health care providers to treat patients.¹ Examples include:

- systems that obtain, archive, and communicate pictures on networks within health care facilities, such as computed tomography, magnetic resonance, ultrasound, nuclear medicine, and endoscopy systems;
- systems that monitor patient activity, such as electrocardiographic systems; and
- systems that communicate with clinical laboratory analyzers, such as laboratory information systems.²

One expert estimates that a large hospital might have around 85,000 medical devices connected to its network.³ Although they are distinct from hospitals' electronic health record (EHR) systems, these devices may connect to the same network as a hospital's EHR system, and thus can be connected to the EHR system as well as to other devices on the same network. As a result, networked devices that lack proper cybersecurity may have vulnerabilities that could lead to adverse outcomes. For example, in May 2017, the WannaCry ransomware attack affected radiological devices in some hospitals—the first known ransomware attack to affect networked medical devices.⁴ According to an August 2017 media report, two in five health care providers said that despite the risk, their respective organizations took no steps to prevent attacks on medical devices.⁵ See Exhibit 1 for an illustration of how networked devices could be connected to other health information technology on a hospital's network.

Cyberattacks on hospitals increased in 2020. In Germany, the first death resulting from a ransomware attack occurred in September 2020 when an attack forced a hospital to turn away a patient in need of critical care.⁶ In the United States, Universal Health Services, which operates about 400 facilities, was the victim of a cyberattack in September 2020 that resulted in an outage of health information technology over multiple days.⁷ In October 2020, the Department of Health and Human Services (HHS) and the Federal Bureau of Investigation warned of increased and imminent ransomware attacks on hospitals.⁸ Following this warning, researchers observed a 45-percent increase in attacks against health care organizations, which was more than double the average increase seen across other industries.^{9,10}

Exhibit 1: Illustration of how networked devices connect to other health information technology on a hospital's network



The safeguards necessary to protect networked medical devices from cyberattacks could fit within hospitals' broader cybersecurity frameworks. Thus, safeguards might include plans for managing software updates and patching on devices themselves, but also other approaches, such as network segmentation (i.e., dividing one network into smaller parts to improve security). To develop their cybersecurity frameworks, hospitals may follow guidance developed by an organization such as the National Institute of Standards and Technology (NIST), a nonregulatory agency of the Department of Commerce; or the Health Information Trust Alliance (HITRUST), a private company. Regardless of what guidance a hospital follows, each hospital's framework should be based on its unique set of circumstances and risks. Furthermore, no one safeguard alone can ensure cybersecurity and each comes at a cost to hospitals.

Medicare Oversight of Medicare-Participating Hospitals

To ensure that hospitals meet its minimum requirements, the Centers for Medicare & Medicaid Services (CMS) relies on State survey agencies and Medicare accreditation organizations (AOs) to inspect Medicare-participating hospitals through onsite surveys every 3 years, generally. When State agencies conduct surveys, they follow CMS's survey protocol, which does not specifically require hospitals to have any cybersecurity protections for their networked devices. In 2017, CMS sent a memo to State survey agency directors that encouraged—but did not require—providers to consider cybersecurity as an element in the development of their emergency plans.¹¹

Instead of undergoing a survey by a State survey agency, about 85 percent of hospitals choose to demonstrate compliance with CMS's standards by earning accreditation from an AO.¹² Like State survey agencies, AOs conduct onsite surveys to assess Medicare-participating hospitals' compliance with Medicare's requirements. However, AOs follow their own survey protocols. The Social Security Act requires AOs' survey protocols to be equivalent to or more stringent than those of CMS.¹³ CMS oversees the AOs by reviewing their survey protocols and conducting complaint investigations and random validation surveys for hospitals that AOs have surveyed.¹⁴ CMS has approved four AOs to accredit hospitals for participation in Medicare: The Joint Commission (TJC); the Healthcare Facilities Accreditation Program (HFAP); DNV (formerly known as DNV GL, which was formed from the merger of Det Norske Veritas and Germanischer Lloyd); and the Center for Improvement in Healthcare Quality (CIHQ).

The Medicare Conditions of Participation and Interpretive Guidelines






The 23 Conditions of Participation (CoPs) cover a wide array of topics and set forth the minimum health and safety requirements (called standards) for acute-care hospitals that wish to participate in the Medicare program. To help surveyors understand how to interpret the CoPs, CMS also publishes a survey protocol called the Interpretive Guidelines. Each CoP typically includes a set of Interpretive Guidelines, offering details and examples for surveyors to use in assessing hospital compliance. Several CoPs are potentially relevant to hospitals' taking proper cybersecurity precautions with networked medical devices, including the CoPs on physical environment; emergency preparedness; patients' rights and privacy; medical records; and compliance with all applicable Federal, State, and local laws. See Exhibit 2 for a description of these CoPs.

The Interpretive Guidelines for these CoPs may include additional guidance related to cybersecurity, albeit limited to the security of protected health information. The Interpretive Guidelines for the patients'-rights CoP include hospitals' use of "passwords and other security measures on computers maintaining personally identifiable health information."¹⁵ The Interpretive Guidelines for the medical-records CoP speak to the "security and protection" of patients' electronic health records. With regard to the emergency-preparedness CoP, CMS updated several of the requirements in 2019 as part of an effort to reduce provider burden and increase flexibility.¹⁶

CMS also requires hospitals to comply with parts of the Life Safety Code, a compilation of safety requirements published every 3 years by the National Fire Protection Association (NFPA). The specific code for health care facilities is known as NFPA 99. CMS adopted the 2012 edition of NFPA 99 in 2016. However, CMS excluded from its requirements the NFPA 99 chapter that specifically mentions cybersecurity. CMS asserted that it "ha[s] no authority to regulate these specific

topics in health care facilities,” and that the chapter is “not within the scope of the conditions of participation”¹⁷

Exhibit 2: Description of CoPs With Potential Cybersecurity Relevance

	PHYSICAL ENVIRONMENT § 482.41	Hospitals must maintain facilities, supplies, and medical equipment to ensure an acceptable level of safety and quality.
	EMERGENCY PREPAREDNESS § 482.15	Hospitals must plan for disasters and emergencies, including cyberattacks, using an all-hazards approach.
	PATIENT RIGHTS § 482.13	Hospital must protect patients’ right to personal privacy and the confidentiality of paper and electronic records.
	MEDICAL RECORDS § 482.24	Hospitals must prevent unauthorized access to confidential medical records.
	FEDERAL, STATE, & LOCAL LAWS § 482.11	Hospitals must comply with all applicable Federal, State, and local laws.

Other HHS Agencies with a Role in Cybersecurity of Medical Devices

Several HHS agencies and offices have roles that involve cybersecurity. These agencies and offices include the Office for Civil Rights, the Food and Drug Administration (FDA), the Office of the National Coordinator for Health Information Technology, and the Health Sector Cybersecurity Coordination Center.

The Office for Civil Rights is responsible for enforcing the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA).¹⁸ This rule establishes safeguards to assure the confidentiality, integrity, and availability of individuals’ electronic protected health information, including such information used in networked medical devices.^{19, 20} HIPAA also requires hospitals to conduct risk assessments, contingency planning, and other activities that may align with the CoPs.²¹ The Office for Civil Rights investigates complaints and performs compliance reviews in response to breach notifications.²²

Since 2011, the Office for Civil Rights has conducted audits to assess providers’ compliance with the Security Rule. In these audits, it reviews the policies and procedures that providers employed to meet selected standards and HIPAA implementation specifications.²³ In 2020, the Office for Civil Rights released the results of audits it conducted in 2016 and 2017 of 166 covered entities (i.e., health care providers, health plans, and health care clearinghouses). These audits found that

most entities met timeliness requirements for providing HIPAA-related breach notifications to individuals. However, the audits also found that most entities failed to adequately safeguard protected health information and that they struggled to implement the Security Rule's requirements for risk analysis and risk management.²⁴

The Food and Drug Administration (FDA) regulates medical devices throughout their entire product life cycles, from premarket approval to postmarket availability and use. Once FDA approves or clears a device to enter the market, it conducts postmarket surveillance to ensure that there are no unexpected safety or effectiveness concerns that emerge once the device is marketed.²⁵ FDA considers cybersecurity for networked medical devices to be a responsibility shared among stakeholders, including FDA, device manufacturers, and health care providers.²⁶

Two other offices within HHS also have a role in cybersecurity. First, the Office of the National Coordinator for Health Information Technology makes available tools and guidance for providers related to securing protected health information.²⁷ Finally, HHS's Health Sector Cybersecurity Coordination Center develops cyberattack mitigation resources and fosters collaboration and partnerships across entities in health care and public health.²⁸

Previous Office of Inspector General (OIG) work

OIG has previously examined FDA's role in assessing the cybersecurity risk of medical devices in both premarket and postmarket settings. A 2018 report found that FDA had taken steps to address emerging cybersecurity concerns, including issuing guidance documents on medical device cybersecurity to FDA reviewers of devices, and reviewing cybersecurity information in premarket submissions for networked medical devices. However, the report also found that FDA could do more to integrate its assessment of cybersecurity for networked medical devices into its premarket review process. OIG recommended that FDA do the following: promote the use of presubmission meetings to address cybersecurity-related questions and include cybersecurity in tools that FDA reviewers use to facilitate their reviews of networked devices.²⁹ FDA concurred with and implemented these recommendations.

Another 2018 report found that FDA's policies and procedures were insufficient for handling postmarket events involving cybersecurity of medical devices. The report found that FDA had not adequately tested its ability to respond to emergencies resulting from cybersecurity events with medical devices. In addition, the report found that in 2 of 19 district offices, FDA had not established written standard operating procedures to address recalls of medical devices vulnerable to cybersecurity threats. OIG recommended that FDA assess cybersecurity risks to medical devices; enter into a formal agreement with Federal partners; ensure creation of procedures for recalls of devices vulnerable to cybersecurity threats; and establish procedures for sharing information with key stakeholders about cybersecurity events. FDA concurred with the recommendations and has implemented all but the last.³⁰

RESULTS





The CoPs do not include requirements for the cybersecurity of networked devices, and the AOs do not use their discretion to require hospitals to have such cybersecurity plans

AOs' requirements must meet or exceed those of the CoPs, and the CoPs do not include any requirements for the cybersecurity of networked devices.³¹ This means that CMS does not expect or require AOs to ask hospitals about the methods they use to secure networked devices from cyberattacks. AOs told us they base their hospital requirements on the CoPs and look to CMS for guidance about how to assess hospital compliance with the requirements. Therefore, the AOs do not require hospitals to have a plan for networked device cybersecurity. Such a requirement would allow the AOs to consistently and routinely review hospitals' cybersecurity protections for their networked devices.

However, AOs sometimes review limited aspects of networked device cybersecurity under certain circumstances

Without a consistent requirement across AOs to review networked devices for cybersecurity, such reviews are likely to happen only under certain circumstances. During their surveys of hospitals, AOs review a wide range of hospital operations, records, and equipment in a short timeframe, covering 23 CoPs. Some aspects of those reviews could spur attention to device cybersecurity. However, only TJC's survey protocol specifically prompts surveyors to ask about device cybersecurity in response to certain topics emerging during interviews with hospital staff. Thus, standard procedure does not drive whether the cybersecurity of networked devices comes up. See Exhibit 3 for a list of CoPs that AOs told us they use when reviewing cybersecurity of networked devices.

Exhibit 3: How AOs told us they apply the CoPs to review the cybersecurity of networked devices

	Relevant Standards and CoPs	How AOs could apply the CoP to review the cybersecurity of networked medical devices
	PHYSICAL ENVIRONMENT Medical Equipment § 482.41(d)	Two AOs verify that facilities, supplies, and equipment (including networked medical devices) are maintained to ensure an acceptable level of safety and quality.
	EMERGENCY PREPAREDNESS Risk Assessment, Planning, Policies, Training § 482.15(a, b, d)	AOs verify that the hospital has a comprehensive emergency preparedness program with risk assessment and with planning, policies, and procedures, including with regard to risk to networked medical devices.
	PATIENT RIGHTS Protecting privacy, safety, and confidentiality § 482.13(c-d)	AOs review controls protecting the privacy and confidentiality of patient records.
	MEDICAL RECORDS Preventing unauthorized access § 482.24(b)	AOs complete a high-level review of the policies and procedures in place to protect the security and integrity of EHRs.

Two of the four AOs have requirements for equipment maintenance that may yield limited insight into device cybersecurity

Opportunity exists within the medical-equipment standard of the physical environment CoP for AOs to draw attention to device cybersecurity. Two of the four AOs—DNV and TJC—told us that they linked that standard to device cybersecurity, albeit in limited ways.


When DNV draws on the medical-equipment standard to make the connection to cybersecurity, its approach is limited. DNV’s standards and survey protocols do not explicitly direct surveyors to assess the extent to which hospitals comply with manufacturers’ cybersecurity-related recommendations, which could include patching schedules and security settings. Rather, they require hospitals to establish a medical-equipment management system to address serious injuries or deaths related to medical equipment, as well as equipment problems and failures. During surveys, DNV surveyors review maintenance records for a sample of medical equipment, including device types that are usually networked. They then determine for that sample whether the hospital records and investigates equipment failures and downtime and whether it adheres to manufacturers’ maintenance recommendations (including recalls).

Likewise, TJC requires hospitals to have some means to monitor medical-equipment recalls and alerts, including those that involve cybersecurity, such as a software problem. For example, a hospital might subscribe to device recall and alert

notifications from the ECRI Institute, a nonprofit health care research organization, to fulfill this requirement. Those recalls and alerts may or may not concern cybersecurity.

If hospitals identify networked device cybersecurity as part of their emergency-preparedness risk assessments, AOs will review the hospitals' mitigation plans

Hospitals have an opportunity to elevate networked device cybersecurity as part of their all-hazards risk planning. CMS's emergency-preparedness standards require hospitals to complete risk assessments—in the form of hazard vulnerability analyses—as part of the hospitals' all-hazards emergency-preparedness planning.³² Using an all-hazards approach for risk planning enables hospitals to identify, prepare for, and develop the capacity to address the full spectrum of the emergencies or disasters that are most likely to impact a facility.³³ These can include pandemic influenza, major earthquakes, major hurricanes, and terrorist attacks, among others.³⁴ As part of this planning, hospitals may also identify networked device cybersecurity as a top concern. AOs told us that in practice, however, hospitals did not identify device cybersecurity as part of their risk assessments very often.



ALL-HAZARDS APPROACH

- Encourages adequate planning for both natural and manmade disasters
- Builds preparedness for a full spectrum of emergencies or disasters
- Is an integrated approach to emergency preparedness planning
- Is part of a shift in focus in emergency management from response to preparedness and mitigation
- Was incorporated into CMS guidance by 2016 emergency preparedness requirements
- Includes cybersecurity events, per CMS's Interpretive Guidelines

Although CMS allows hospitals to self-identify concerns, three AOs—TJC, DNV, and HFAP—require that hospitals consider cybersecurity when conducting their risk planning. DNV and HFAP require hospitals to comply with the National Fire Protection Association's 2012 codes and standards in their entirety, including chapters that CMS excludes from its regulations and Interpretive Guidelines. One of these chapters prompts hospitals to consider cybersecurity—but not specifically networked device cybersecurity—in their risk planning. TJC's surveyor protocol also prompts surveyors to ask—during the orientation and emergency management portions of the onsite survey—about

a hospital's risk awareness, detection, and response with regard to cyberemergencies.

If a hospital lists cybersecurity as a top concern on its hazard vulnerability analysis, the hospital must have written emergency-preparedness policies and procedures to reduce and mitigate the risk of any identified cybersecurity vulnerabilities, which may or may not include risks to networked medical devices.³⁵ Each of the AOs told us (or provided standards showing) that they verify that hospitals conducted a hazard vulnerability analysis. Three of the AOs further stated that they also examine the

related plans and procedures for prevention, preparation for, and mitigation of the risks that hospitals identified in their vulnerability analyses.

However, without hospitals' identifying cybersecurity as a top concern, AOs will not be prompted to raise it with them. AOs reported observing varying levels of hospitals' listing cybersecurity as a top concern. One AO told us that 20 to 25 percent of hospitals listed it, whereas another told us that very few hospitals did so. As a result, AOs are unlikely to discuss it with many of the hospitals they survey.

Assessing hospital safeguards for the privacy and confidentiality of medical records may prompt AOs to examine networked devices

The CoPs on medical records and patients' rights represent another potential avenue for AOs to review device cybersecurity—after all, many networked devices connect directly to hospitals' EHR systems. The AOs, however, report that their focus is more on EHR systems' safeguards for protecting privacy and confidentiality. For example, AOs commonly paid attention to passwords, encryption, and access monitoring. Such safeguards are critically important, but they are not directed to networked device cybersecurity.

Nonetheless, one AO—HFAP—hypothesized that networked devices could come under scrutiny during its review of medical records. HFAP noted that an EHR system is “not necessarily a stand-alone resource, it has all kinds of things feeding into it,” including various networked devices. Therefore, surveyors could examine those devices if they observed frequent problems with EHRs missing data. However, HFAP also noted that hospitals are vigilant about safeguarding patient records, limiting the likelihood of examining networked devices in any detail.

CMS and the AOs do not plan to update their survey requirements to address networked device cybersecurity or cybersecurity generally

To date, neither CMS nor AOs have plans to update their approaches to oversight of hospitals' cybersecurity in general or of networked device cybersecurity specifically. CMS stated that it does not plan to revise the CoPs or Interpretive Guidelines to address preventive cybersecurity. CMS noted that it requires hospitals to comply with the physical-environment CoP, which requires hospitals to maintain facilities, supplies, and equipment to ensure an acceptable level of safety and quality. Thus, according to CMS, a hospital must maintain its networked devices in a manner that ensures an acceptable level of safety and quality for patients, including an acceptable and standard level of cybersecurity.

None of the AOs plan to add a requirement for networked device cybersecurity to their survey protocols. Some AOs emphasized CMS's role in influencing changes to

AOs' hospital survey protocols. DNV would include device-specific requirements only if CMS added a new requirement to the CoPs. If CMS were to establish a requirement for networked device cybersecurity, CIHQ emphasized the need for training and guidance for AOs to assess hospital compliance with the requirement.

AOs cited challenges that could limit their ability to effectively oversee networked device cybersecurity. One such challenge was the AOs' ability to apply cybersecurity standards to health care. Although external cybersecurity frameworks exist, some AOs expressed doubts as to their suitability for hospitals. Another challenge was AOs' capacity to assess hospitals' cybersecurity practices. Because surveyors are not cybersecurity experts, AOs were concerned about their ability to assess the sufficiency of hospitals' cybersecurity defenses.

CONCLUSION AND RECOMMENDATION

As health care delivery becomes more reliant on technology, cyberattacks on hospitals continue to increase. Hospitals represent a broad target for cyberattacks, and attackers could gain access to a hospital's entire network via a hacked device. In 2020, a major American health care provider suffered a multiday outage of its health information technology because of a cyberattack, and the Federal Government warned of increased ransomware attacks on hospitals. Therefore, it is more important than ever that hospitals have a plan for securing their networked devices—which can number in the tens of thousands in a large organization—before those devices are compromised in a cyberattack.

Yet CMS's CoPs are silent on networked device cybersecurity as well as cybersecurity in general. Accordingly, AOs—whose requirements must meet but also may exceed those of the CoPs—rarely use their discretion to examine the cybersecurity of networked devices during their hospital surveys. As a result, Medicare lacks consistent oversight of the cybersecurity of networked devices in hospitals.

CMS told us that it is revising the Interpretive Guidelines for both the emergency-preparedness CoP and the physical-environment CoP, but it said that its timeframes have been delayed because of the COVID-19 pandemic. Although CMS does not plan to address cybersecurity of networked devices in this revision, we ask that it reconsider. CMS has the opportunity to underscore the importance of cybersecurity to ensuring that patients receive safe and high-quality health care. Furthermore, CMS could draw on the expertise of other agencies within HHS, such as FDA or the Office for Civil Rights, to ensure that hospitals are good stewards of cybersecurity.

We recommend that CMS:

Identify and implement an appropriate way to address cybersecurity of networked medical devices in its quality oversight of hospitals, in consultation with HHS partners and others

CMS could use the Interpretive Guidelines to draw attention to cybersecurity of networked medical devices. It could do so by identifying in the Interpretive Guidelines the CoP or CoPs whose scope includes cybersecurity of networked devices. In those parts of the Interpretive Guidelines, CMS could add questions for surveyors to probe with or nonbinding guidance that points to cybersecurity resources. The Interpretive Guidelines for pharmaceutical services—in which CMS points to

nonbinding guidance in several places—can serve as a model for this approach. We recognize that it is not reasonable to expect surveyors to have the expertise of cybersecurity professionals, nor to directly test the security of networked devices. However, AOs' surveys already include some activities related to cybersecurity of networked devices that do not require such specialized expertise. CMS can use these activities to inform its changes.

For example, CMS could:

- Create language stating that CMS considers cybersecurity as part of keeping devices in safe operating condition (in the physical-environment CoP's standard for equipment maintenance.)
- Highlight the risk that unsecured devices connected to a hospital's EHR system pose to protected health information (in the CoPs for patient rights and medical records).
- Instruct surveyors to ask hospitals if they considered cybersecurity of networked devices when they conducted their hazard vulnerability analyses, as CMS has previously encouraged. The guidelines could contain additional probe questions, including on networked devices, to help surveyors gauge the robustness of hospitals' hazard vulnerability analyses (in the emergency-preparedness CoP). CMS could also go further and state that it expects cybersecurity to be a part of every hospital's emergency planning.
- Remind hospitals to maintain compliance with HIPAA requirements, including the Security Rule (in the CoP on Federal, State, and local laws). This rule establishes safeguards to assure the confidentiality, integrity, and availability of individuals' electronic protected health information, including such information used in networked medical devices.

Alternatively, if CMS determines that the existing CoPs are insufficient, it could add standards to existing CoPs, or create a new CoP specifically focused on cybersecurity. It could then include requirements for networked device cybersecurity in this new CoP and reference them in the Interpretive Guidelines. We acknowledge that this option would require CMS to follow the rulemaking process and would thus be a lengthier and more burdensome process than just amending the Interpretive Guidelines.

Whichever option CMS chooses, it should work with partners both inside and outside HHS to determine the best method for addressing cybersecurity of networked medical devices in hospitals. Within HHS, those partners include FDA, the Office for Civil Rights, and the Health Sector Cybersecurity Coordination Center. Outside HHS, those partners include NIST, the Health Information Trust Alliance (HITRUST), and the AOs. Each of these partners has different expertise that CMS could leverage—FDA, on networked devices and device manufacturers; the Office for Civil Rights, on safeguarding protected health information; NIST and HITRUST, on up-to-date, scalable frameworks for health care organizations; and the AOs, on their experience surveying a wide array of hospitals.

Any of these options would be an important first step towards helping ensure a consistent approach to overseeing cybersecurity of networked devices in hospitals.

AGENCY COMMENTS AND OIG RESPONSE

CMS stated that it “concur[red] with considering additional ways to appropriately highlight the importance of cybersecurity of networked medical devices for providers in consultation with its HHS partners that have specific oversight authority regarding cybersecurity.” In its comments, CMS highlighted the all-hazards approach of the CoPs’ emergency-preparedness requirements and said that emergencies may include cyberattacks. It also pointed to past efforts to educate providers on cybersecurity.

We acknowledge CMS’s past efforts to highlight the importance of cybersecurity. However, CMS’s proposed action would not implement our recommendation because it does not commit the agency to changing its quality oversight. We continue to recommend that CMS identify and implement an appropriate way to address cybersecurity of networked medical devices in its quality oversight of hospitals, in consultation with HHS partners and others. We look forward to CMS’s sharing, in its Final Management Decision, its plan for addressing cybersecurity of networked medical devices under its own authority for quality oversight of hospitals. Cybersecurity is an increasingly pressing patient safety issue, and it is important that it be reflected in CMS’s quality oversight.

See Appendix A for the full text of CMS’s comments.

METHODOLOGY

Scope

This inspection is national in scope, including CMS and the four AOs that accredit acute-care hospitals that participate in Medicare. It covers their survey protocols and/or planned changes to their processes as of summer 2020. The devices covered by this inspection are devices regulated by FDA as medical devices that support wired or wireless connectivity to a hospital network. This inspection excludes devices that patients use outside of a hospital setting, such as pacemakers. This inspection also excludes State survey agencies. These entities use CMS's survey protocols, which are publicly available, whereas AOs' survey protocols are proprietary and not publicly available.

Data Collection

We conducted structured telephone interviews with knowledgeable staff at the four AOs during July and August of 2020. We asked AO staff the extent to which their survey standards required hospitals to have a cybersecurity plan for networked devices as well as other ways in which their surveys might cover the cybersecurity of networked devices. We requested documentation of relevant survey standards from the AOs. We also submitted written questions to CMS inquiring as to any planned changes to the CoPs.

Data Analysis

We analyzed our interview data and identified common themes across the AOs. Where possible, we verified the interview data with the AOs' survey standards.

Limitations

We did not independently verify all the information from our AO interviews.

Standards

We conducted this study in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.



AGENCY COMMENTS

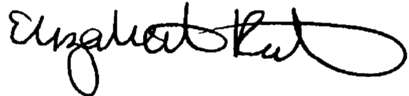
DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

Date: May 11, 2021

To: Suzanne Murrin
Deputy Inspector General
Office of Inspector General

From: Elizabeth Richter
Acting Administrator
Centers for Medicare & Medicaid Services 

Subject: Office of Inspector General Draft Report: Medicare Lacks Consistent Oversight of Networked Medical Device Cybersecurity in Hospitals OEI-01-20-00220

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report. CMS is committed to improving quality of care for patients through appropriate oversight of hospital safety.

Hospitals are required to be in compliance with the Federal requirements set forth in the Medicare Conditions of Participation (CoPs) in order to receive Medicare payments. As part of CMS's efforts to oversee hospital compliance with federal requirements, CMS works in partnership with State Survey Agencies (SSAs) and Accrediting Organizations (AOs) to conduct onsite hospital surveys. These surveys are accomplished through observations, interviews, and document/record reviews. Surveyors assess the hospital's compliance with the CoPs for all services, areas and locations in which the provider receives payment for patient care services billed under its provider number.

The Medicare CoPs cover a wide array of topics, including an emergency preparedness requirement that directs hospitals to implement an all-hazards approach, which is an integrated approach to emergency preparedness planning that focuses on capacities and capabilities that are critical to preparedness for a full spectrum of emergencies or disasters. This approach is specific to the location of the provider and considers the particular type of hazards most likely to occur in their areas. These may include, but are not limited to, care-related emergencies, equipment and power failures, and interruptions in communications, including cyberattacks. Specifically, it is important that hospitals develop, implement and maintain an effective antiviral computer software program to prevent malware viruses from cyberattacks.

Hospitals are required to review and update their emergency preparedness plan at least biennially. CMS encourages providers to consider cybersecurity as an element in the development of their emergency plans, risk assessments, and annual testing exercises. While not a requirement, facilities may consider adding cybersecurity protocols to their policies and procedures. Additionally, given the requirement for facilities to establish communication plans, which also includes alternate means of communication, the facility could consider addressing

within their policies and procedures an element of how to communicate with staff and different departments in the event computers or other means of communication are inaccessible. In a guidance document, S&C: 17-17-All released in 2017, CMS made recommendations to providers regarding cybersecurity and provided several resources for facilities to use to assist in their overall cybersecurity awareness. For example, in the guidance, CMS provided links to the Food and Drug Administration's information specifically related to cybersecurity of networked medical devices. In addition, if hospitals reach out to the agency with inquiries related to cybersecurity, CMS connects them with the Health and Human Services healthcare emergency preparedness information gateway, ASPR TRACIE, which has a dedicated topic collection on guidance for cybersecurity in healthcare. Lastly, CMS also intends to continue to provide education to providers when appropriate, such as the "*Overview of 405d Publication – Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)*," which was presented at the HIMSS19 conference in 2019.

CMS thanks the OIG for its efforts on this issue and looks forward to working collaboratively on this and other issues in the future. OIG's recommendations and CMS' responses are below.

OIG Recommendation

Identify and implement an appropriate way to address cybersecurity of networked medical devices in its quality oversight in hospitals, in consultation with HHS partners and others.

CMS Response

CMS concurs with considering additional ways to appropriately highlight the importance of cybersecurity of networked medical devices for providers in consultation with its HHS partners that have specific oversight authority regarding cybersecurity.

ACKNOWLEDGMENTS AND CONTACT

Acknowledgments

Ivan Troy served as the team leader for this study. Others in the Office of Evaluation and Inspections who conducted the study include Caitlin Foster and Rachel Pavia. Office of Evaluation and Inspections staff who provided support include Joe Chiarenzelli, Kevin Farber, and Christine Moritz.

This report was prepared under the direction of Joyce Greenleaf, Regional Inspector General for Evaluation and Inspections in the Boston regional office, and Kenneth Price, Deputy Regional Inspector General.

Contact

To obtain additional information concerning this report, contact the Office of Public Affairs at Public.Affairs@oig.hhs.gov. OIG reports and other information can be found on the OIG website at oig.hhs.gov.

Office of Inspector General
U.S. Department of Health and Human Services
330 Independence Avenue, SW
Washington, DC 20201

ENDNOTES

¹ Food and Drug Administration (FDA), "Cybersecurity," October 22, 2020. Accessed at <https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity> on December 15, 2020.

² FDA, "Information for Healthcare Organizations about FDA's 'Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software'," February 2005. Accessed at <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/information-healthcare-organizations-about-fdas-guidance-industry-cybersecurity-networked-medical> on December 15, 2020.

³ Elizabeth O'Dowd, "Considerations for Deploying Healthcare Wireless Networks," *HIT Infrastructure*, February 3, 2017. Accessed at <https://hitinfrastructure.com/features/considerations-for-deploying-healthcare-wireless-networks> on June 1, 2020.

⁴ Thomas Brewster, "Medical Devices Hit by Ransomware for The First Time In US Hospitals," *Forbes*, May 17, 2017. Accessed at <https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#1fedcfad425c> on March 2, 2020. FDA, "Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication," August 29, 2017. Accessed at <https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals> on March 2, 2020.

⁵ Hannah Kuchler, "Medical Device Makers Wake Up to Cyber Security Threat," *Financial Times*, August 1, 2017. Accessed at <https://www.ft.com/content/00989b9c-7634-11e7-90c0-90a9d1bc9691> on March 5, 2020.

⁶ Associated Press, "German Hospital Hacked, Patient Taken to Another City Dies," September 17, 2020. Accessed at <https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94> on October 27, 2020.

⁷ Kat Jerich, "UHS Hospital Chain Hit with Apparent Ransomware Attack," *Healthcare IT News*, September 29, 2020. Accessed at <https://www.healthcareitnews.com/news/uhs-hospital-chain-hit-massive-ransomware-attack> on November 2, 2020.

⁸ Cybersecurity and Infrastructure Security Agency, *Joint Cybersecurity Advisory, Ransomware Activity Targeting the Healthcare and Public Health Sector*, October 28, 2020. Accessed at [https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20Activity Targeting the Healthcare and Public Health Sector.pdf](https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20Activity%20Targeting%20the%20Healthcare%20and%20Public%20Health%20Sector.pdf) on March 2, 2021.

⁹ Jessica Davis, "Healthcare Accounts for 79% of All Reported Breaches, Attacks Rise 45%," *Health IT Security*, January 5, 2021. Accessed at <https://healthitsecurity.com/news/healthcare-accounts-for-79-of-all-reported-breaches-attacks-rise-45> on January 13, 2021.

¹⁰ Check Point Software Technologies Ltd, "Attacks Targeting Healthcare Organizations Spike Globally as COVID-19 Cases Rise Again," *Check Point Blog*. Accessed at <https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/> on June 10, 2021.

¹¹ CMS, *Recommendations to Providers Regarding Cybersecurity*, Ref: S&C: 17-17-ALL, January 13, 2017. Accessed at <https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Downloads/Survey-and-Cert-Letter-17-17.pdf> on March 5, 2021.

¹² Centers for Medicare and Medicaid Services (CMS), *FY 2018 Report to Congress (RTC): Review of Medicare's Program Oversight of Accrediting Organizations (AOs) and the Clinical Laboratory Improvement Amendments of 1988 (CLIA) Validation*

Program, August 20, 2019. Accessed at <https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Downloads/QSO-19-17-AO-CLIA.pdf> on March 2, 2020.

¹³ Social Security Act, § 1865(a)(1).

¹⁴ CMS, *Review of Medicare's Program for Oversight of Accrediting Organizations and The Clinical Laboratory Improvement Validation Program Fiscal Year 2018 Report to Congress*. Accessed at <https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Policy-and-Memos-to-States-and-Regions-Items/QSO-19-17-AO-CLIA> on March 27, 2020.

¹⁵ CMS, *State Operations Manual, Appendix A—Survey Protocol, Regulations and Interpretive Guidelines for Hospitals* (Rev. 200, 02.21.20), A-0143 (Rev. 95, Issued: 12-12-13, Effective: 06-07-13, Implementation: 06-07-13), § 482.13(c)(1)—The patient has the right to personal privacy. Interpretive Guidelines § 482.13(c)(1). Accessed at https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/som107ap_a_hospitals.pdf on January 21, 2021.

¹⁶ 84 Fed. Reg. 51732 (Sept. 30, 2019).

¹⁷ CMS, *Final Rule: Medicare and Medicaid Programs; Fire Safety Requirements for Certain Health Care Facilities*, 81 Fed. Reg. 26872 (May 4, 2016). Specifically, see 26887-9 and 26894: CMS excludes NFPA 99 2012 chapters 7—Information Technology and Communications Systems for Health Care Facilities; 8—Plumbing; 12—Emergency Management; and 13—Security Management.

¹⁸ HHS, *Summary of the HIPAA Security Rule*. Accessed at <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html> on February 26, 2021.

¹⁹ 45 CFR pts. 160 and 164, subpts. A, C, and E.

²⁰ The Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009 further strengthened the civil enforcement of the HIPAA rules. HITECH Act § 13410.

²¹ 45 CFR §§ 164.308(a)(1)(ii)(A) and 164.308(a)(7).

²² HHS Office for Civil Rights, *Enforcement of Privacy and Security Rules*. Accessed at <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html> on February 25, 2020.

²³ HHS Office for Civil Rights, *HIPAA Privacy, Security, and Breach Notification Audit Program*. Accessed at <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html> on March 5, 2020.

²⁴ HHS Office for Civil Rights, *2016-2017 HIPAA Audits Industry Report*, December 2020. Accessed at <https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf> on January 13, 2021.

²⁵ FDA, *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health*. Accessed at <https://www.fda.gov/media/112497/download> on February 26, 2021.

²⁶ OIG, *FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Review Process for Medical Devices* (OEI-09-16-00220), September 2018.

²⁷ Office of the National Coordinator for Health Information Technology, *Health IT Privacy and Security Resources for Providers*. Accessed at <https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers> on January 13, 2021.

²⁸ Healthcare Cybersecurity Coordination Center, *HC3 About Us*. Accessed at <https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf> on January 13, 2021.

²⁹ OIG, *FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Review Process for Medical Devices* (OEI-09-16-00220), September 2018.

³⁰ OIG, *The Food and Drug Administration's Policies and Procedures Should Better Address Postmarket Cybersecurity Risk to Medical Devices* (A-18-16-30530), October 2018.

³¹ Social Security Act, § 1865(a)(1).

³² 42 CFR §§ 482.15; Appendix Z. Emergency preparedness planning under CMS's requirements is separate from contingency planning under the HIPAA Security Rule's requirements, but the two activities are complementary and could feed into one another.

³³ 42 CFR § 482.15.

³⁴ Federal Emergency Management Agency, *National Planning Scenarios Fact Sheet*. Accessed at https://www.fema.gov/txt/media/factsheets/2009/npd_natl_plan_scenario.txt on October 19, 2020.

³⁵ 42 CFR § 482.15(b).