PUBLIC COMMENT: FOUNDATION FOR DEFENSE OF DEMOCRACIES

Department of Health and Human Services
Centers for Medicare & Medicaid Services

Request for Information: Increasing Health Care Resiliency

[42 CFR 403, 422, 431, 438, 440, 457, 45 CFR 156, 162, 170. Docket No. CMS-0062-P]

AUTHORS

Annie Fixler
Director and Senior Fellow, FDD's Center on Cyber and Technology Innovation

Sophie McDowall
Research Associate, FDD's Center on Cyber and Technology Innovation

Aarushi Garg
Research Intern, FDD's Center on Cyber and Technology Innovation

Washington, DC
June 15, 2026

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Despite the critical role they play in maintaining public health, safety, and wellbeing, health care providers are often under-equipped to handle cybersecurity challenges that threaten the delivery of critical services. The challenge is widespread — chronic underinvestment and structural vulnerability contribute to the threat environment, while attacks from ransomware groups have cost the health care sector millions of dollars and disrupted care for hundreds of thousands of patients.[1] Addressing the gaps requires an understanding of the threat landscape, sector vulnerabilities, and potential paths forward to secure the sector and protect patients and providers alike.

While the Department of Health and Human Services' (HHS's) Centers for Medicare and Medicaid Services (CMS) does not have regulatory oversight of all hospitals and health care entities, its unique position as a standards-setting body for those providing Medicare and Medicaid services provides an opportunity to guide the adoption of strong cybersecurity practices that can equip providers to keep their patients, practices, and finances safe.

Cyber Risks Threaten Health Care Operations and Impact Patients

America's health care sector is under threat in cyberspace. The United States experienced the most health care-related cyberattacks of any country in 2025, and the FBI has consistently identified the health care and public health sector as the critical infrastructure sector most targeted by ransomware.[2]

When ransomware encrypts a hospital's systems, providers can lose access to electronic health records, diagnostic tools, medication histories, and communication systems. To mitigate the effects of a technology disruption, staff may be forced to revert to manual, paper-based processes for patient triage, exams, and lab requests — practices that are unfamiliar to younger practitioners. In February, for example, a cyberattack on the University of Mississippi Medical Center forced the closure of clinics across the state, causing delays in chemotherapy treatments. At other care centers, staff had to resort to paper documentation.[3]

When a cyberattack hits, patients requiring emergency care may be diverted to other facilities. A 2024 ransomware attack on the Ascension hospital network, which includes 140 hospitals across 19 states, caused multiple hospitals to send ambulances elsewhere.[4]

These impacts contribute to delayed and degraded patient care — sometimes with deadly consequences. Studies of organizations affected by ransomware attacks have found that more than one-third reported increased complications in medical procedures, and nearly a quarter saw

[1] Michael Sugden and Annie Fixler, "Healthcare Cybersecurity Needs a Check Up," *Foundation for Defense of Democracies,* June 2024. (https://www.fdd.org/analysis/2024/06/04/healthcare-cybersecurity-needs-a-check-up)
[2] "FBI: Health Care Was Top Target for Ransomware, Other Cyberthreats in 2025," *American Hospital Association*, April 10, 2026. (https://www.aha.org/news/headline/2026-04-10-fbi-health-care-was-top-target-ransomware-other-cyberthreats-2025)
[3] Sean Lingaas, "Major Cyberattack Forces Closure of Clinics Across Mississippi," *CNN,* February 20, 2026. (https://www.cnn.com/2026/02/20/politics/cyberattack-closes-clinics-mississippi)
[4] Sean Lyngaas, "Cyberattack forces major US health care network to divert ambulances from hospitals," *CNN Business*, May 10, 2024. (https://www.cnn.com/2024/05/10/tech/cyberattack-ascension-ambulances-hospitals)

increased patient mortality.[5] Nearby care centers also experience negative impacts — including longer wait times for patients — as they deal with the influx from the facility suffering the attack.[6] Delays in emergency department admissions as a result of technology disruptions have led to increases in 30-day mortality.[7]

Connected Devices, Legacy Systems, and Third-Party Services Expand the Attack Surface

Hospitals increasingly rely on digitally connected technology across every dimension of operations, from electronic health records and medication dispensing systems to building management, patient monitoring, and diagnostic imaging.[8] However, many of the devices and systems that help providers do their jobs better also introduce risks — each network-connected device is a point for potential compromise, and, according to the sector's own information-sharing and analysis center, health care organizations with more connected devices experience more cyberattacks.[9]

The concern about compromised devices stems not only from malicious hackers but also from vulnerabilities intentionally embedded by device manufacturers domiciled in foreign adversary nations. Last year, independent researchers and government officials found that Chinese-manufactured patient monitors deployed in U.S. hospitals were transmitting sensitive patient data to servers in China. These devices contain embedded backdoors, potentially enabling a malicious actor to remotely modify the device.[10] If a medical device were manipulated to display incorrect patient data, providers might administer incorrect treatment. This possibility raises the stakes from data security to patient safety.

Legacy systems represent another entrenched vulnerability. Many internet-connected medical devices, such as wearable monitors, infusion pumps, and imaging systems, run operating systems that no longer receive security updates.[11] When outdated systems no longer receive vendor support, attackers can take advantage of newly discovered exploits while providers are left

---

[5] Rebecca Pifer Parduhn, "Quarter of Providers Saw Mortality Rates Rise After Ransomware Attacks, Survey Finds," *Healthcare Dive,* September 23, 2021. (https://www.healthcaredive.com/news/quarter-providers-mortality-rates-rise-after-ransomware-attack/607095)

[6] Christian Dameff, Jeffrey Tully, Theodore C. Chan, Edward M. Castillo, Stefan Savage, Patricia Maysent, Thomas M. Hemmen, Brian J. Clay, and Christopher Longhurst, "Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US," *JAMA Netw Open*, May 8, 2023. (https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585)

[7] Simon Jones, Chris Moulton, Simon Swift, Paul Molyneux, Steve Black, Neil Mason, Richard Oakley, and Clifford Mann, "Association between delays to patient admission from the emergency department and all-cause 30-day mortality," *Emergency Medicine Journal*, January 18, 2022. (https://emj.bmj.com/content/39/3/168)

[8] Sophie McDowall and Annie Fixler, "Patients Suffer When Hospitals are Unprepared for Cyberattacks," *Foundation for Defense of Democracies,* May 30, 2025. (https://www.fdd.org/analysis/2025/05/30/patients-suffer-when-hospitals-are-unprepared-for-cyberattacks)

[9] "Current and Emerging Healthcare Cyber Threat Landscape," *Health-ISAC and Booz Allen Hamilton Cyber Threat Intelligence*, February 2023, page 7. (https://web.archive.org/web/20230325142734/https://h-isac.org/wp-content/uploads/2023/03/Health-ISAC-Exec-Summary-Annual-Threat-Report_TLP-White-2023.pdf)

[10] Samantha F. Ravich and Johanna Yang, "China Wants Our Hears. Literally." *The Cipher Brief,* June 13, 2025. (https://www.thecipherbrief.com/china-medical-devices)

[11] Maureen Sahualla, "Healthcare Under Siege: Defending Hospitals from IoT Ransomware Attacks," *Cylera*, January 22, 2025. (https://cylera.com/blog/healthcare-iot-ransomware-threats); Mikko Hypponen, "How outdated medical systems leave patient records at risk," *Healthcare Digital*, September 11, 2021. (https://healthcare-digital.com/technology-and-ai/how-outdated-medical-systems-leave-patient-records-risk)

without a fix.[12] When a hospital uses many legacy systems, there is greater potential for vulnerabilities to be discovered and go unpatched. Upgrading legacy infrastructure may be expensive and operationally disruptive, but the cost of failing to do so — measured in financial remediation, reputational impact, and patient harm — can be far greater.[13]

Patching is burdensome, but failing to do so is costly. In February 2023, attackers targeting Lehigh Valley Health Network exploited a known but unpatched vulnerability, causing significant delays in patient care.[14]

Dependence on a few third-party service providers, meanwhile, creates sector-wide fragility. A cyberattack on a single provider can have cascading financial and operational impacts on providers across the country. Clearinghouses are of particular concern. They serve as intermediaries for claims and payment processing between providers and payers, enabling timely payments for medical care. When hackers disrupt the operations of a clearinghouse, they put at risk the financial wellbeing of hospital systems and smaller clinics alike.

The February 2024 ransomware attack on Change Healthcare brought this reality into stark relief. The UnitedHealth Group subsidiary, which processed an estimated 40 percent of all U.S. medical claims, was forced to shut down its systems entirely, halting insurance reimbursements and prescription processing for weeks.[15] Hackers compromised the health care data of nearly 200 million Americans.[16] An American Hospital Association survey of hospitals one month later found that 94 percent suffered a financial impact from the attack and three-quarters reported negative impacts on patient care.[17]

Creating a resilient health care system is not about expecting providers to have redundant clearinghouses or to shift to a different payment platform during a crisis. When providers use clearinghouses, they are required to register in two ways: as a provider in a direct relationship with the clearinghouse and as a provider with a direct relationship with each of the payers from which they plan to accept payment. The diverse payer landscape includes government entities like Medicare, Medicaid, and the Veterans Health Administration, commercial entities like publicly traded insurance companies, and private entities like non-publicly traded insurers and employers.[18] For providers to receive payments through clearinghouses from multiple payers,

---

[12] "How Legacy IT Impacts Healthcare Cybersecurity," *Censinet*, February 9, 2026. (https://censinet.com/perspectives/legacy-it-impacts-healthcare-cybersecurity)
[13] Sahil Kataria, "Legacy System Modernization Cost for Healthcare Providers: 2026 Pricing Guide," *Q Services*, updated May 29, 2026. (https://www.qservicesit.com/pricing/legacy-modernization-cost-for-healthcare-providers); Andrei Zhukouski, "Why healthcare companies can't afford to delay system upgrades," *TYMIQ*, September 4, 2025. (https://www.tymiq.com/post/why-healthcare-cannot-afford-to-delay-system-upgrades)
[14] Lizzie Danielson, "Lehigh Valley Health Network Ransomware Attack," *Huntress,* December 2, 2025 (https://www.huntress.com/threat-library/ransomware/lehigh-valley-health-network-ransomware)
[15] James Rundle, Catherine Stupp, and Kim S. Nash, "Medical Providers Fight to Survive After Change Healthcare Hack," *The Wall Street Journal,* March 1, 2024. (https://www.wsj.com/articles/medical-providers-fight-to-survive-after-change-healthcare-hack-328c2e5a)
[16] Steve Alder, "Healthcare Data Breach Statistics — Updated for 2026," *The HIPAA Journal*, June 4, 2026. (https://www.hipaajournal.com/healthcare-data-breach-statistics)
[17] "AHA Survey: Change Healthcare Cyberattack Having Significant Disruption on Patient Care, Hospitals' Finances," *American Hospital Association*, March 15, 2024. (https://www.aha.org/news/news/2024-03-15-aha-survey-change-healthcare-cyberattack-having-significant-disruptions-patient-care-hospitals-finances)
[18] "Payor," *Definitive Healthcare*, accessed June 5, 2026. (https://www.definitivehc.com/resources/glossary/payor)

they must complete a separate and non-standardized registration process for each entity that they plan to receive payments from. Transitioning to a different clearinghouse to accept or send payments can take weeks to months.[19]

A resilient health care system is not about burdening hospitals with maintaining redundant technology platforms but rather about identifying systemically important technologies, platforms, and entities and ensuring that those systems can maintain minimum viable operations[20] during a crisis to prevent the problem from metastasizing.

Barriers to Cyber Resilience

Technological complexity, financial resource constraints, and workforce gaps all pose challenges to a cybersecure and resilient health care sector. Many providers lack the visibility, tools, or staff to map their own attack surface, much less secure it.

The number and diversity of types of information technology, operational technology, and connected medical devices make securing the perimeter, let alone creating defense-in-depth, challenging for even the most capable health care providers.

Core clinical services compete with administrative and security investments for limited resources, and cybersecurity has consistently lost that competition. Studies indicate that most health care organizations allocate less than 10 percent of their IT budgets to cybersecurity.[21] This underinvestment reflects the financial realities of the sector.

Workforce gaps compound financial limitations. The health care sector faces a significant shortage of qualified cybersecurity professionals. Many organizations lack even a single dedicated IT security professional.[22] This gap is most acute in rural areas, where health care organizations struggle to recruit and retain technical talent. Even when providers recognize the need to invest in cybersecurity, the personnel to implement that investment may be unavailable.

Challenges for Rural Facilities

The impact of a cyberattack can be especially costly in rural areas, where care centers are farther apart.[23] Critical Access Hospitals serve as the only practical emergency care option for the communities around them. When these facilities must divert patients because a ransomware

---

[19] "Switching Clearinghouses," *Chirotouch Community,* accessed June 5, 2026. (https://chirotouch.my.site.com/cloud/s/article/Switching-Clearinghouses)

[20] For a discussion of minimum viable delivery objectives, see: President's Council of Advisors on Science and Technology, "Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World," February 2024. (https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf)

[21] Trustwave, Press Release, "New Trustwave Report Reveals Health Care Security Gaps", October 13, 2025. (https://www.globenewswire.com/news-release/2015/10/13/1109905/0/en/New-Trustwave-Report-Reveals-Health-Care-Security-Gaps.html)

[22] Bill Siwicki, "Black Book: 84% of Hospitals Lack a Dedicated Security Leader," *Healthcare IT News,* December 18, 2017. (https://www.healthcareitnews.com/news/black-book-84-hospitals-lack-dedicated-security-leader)

[23] Sophie McDowall and Annie Fixler, "Patients Suffer When Hospitals are Unprepared for Cyberattacks," *Foundation for Defense of Democracies,* May 30, 2025. (https://www.fdd.org/analysis/2025/05/30/patients-suffer-when-hospitals-are-unprepared-for-cyberattacks)

attack is inhibiting their ability to provide high-quality care, individuals must travel longer distances and wait longer before receiving care. For patients experiencing strokes, heart attacks, or other time-critical emergencies, those additional minutes can be the difference between life and death.[24]

Serving populations that are, on average, older, sicker, and more likely to be uninsured, most rural hospitals operate at a loss.[25] With fewer financial resources, they are less able to invest in cybersecurity defenses, absorb the costs of a ransomware attack, and recover quickly.

Hackers are preying on these under-resourced health care providers. Seventy percent of all successful health care cyberattacks target small health care providers, with dangerous results for the communities they serve.[26] After a cyberattack caused a 14-week system shutdown preventing the facility from submitting insurance claims, St. Margaret's Health in Spring Valley, Illinois, shut its doors.[27] The unrecoverable financial crisis brought to a head by the cyberattack left the community vulnerable. More than 130 rural hospitals have closed nationwide since 2010, and more than 600 are at risk of closing in the near future.[28] While the closures are the result of many different issues, cyberattacks are draining what few resources these hospitals have.

Recommendations

As noted in the request for information, the health care and public health sectors already have several regulations focused on protecting critical data, including the HIPAA Security Rule, FISMA, and the HITECH Act. HHS has also launched multiple efforts focused on cybersecurity — the proposed HIPAA cybersecurity rule, the Office of the National Coordinator for Health Information Technology's (ONC's) SAFER Guides, and the ONC and Office for Civil Rights' Security Risk Analysis tool.

The health care toolkit produced with the Health Sector Coordinating Council and the Cybersecurity and Infrastructure Security Agency (CISA), the sector's cybersecurity performance goals, and the health industry cybersecurity practices each provide valuable guidance to hospitals and other health care providers. The Administration for Strategic Preparedness and Response (ASPR) and the National Institute of Standards and Technology have also produced the Health Care and Public Health Sector Cybersecurity Framework Implementation Guide, and the Federal Trade Commission produced the Start with Security Business Guide for best data practices.

---

[24] Ibid.
[25] Pearl Steinzor, "Health Policy in Crisis: Saving Rural Hospitals Across America," *The American Journal of Managed Care,* August 28, 2024. (https://www.ajmc.com/view/health-policy-in-crisis-saving-rural-hospitals-across-america)
[26] Steve Alder, "Small-Sized and Medium-Sized Healthcare Providers Most Likely to Be Attacked with Ransomware," *The HIPAA Journal,* April 16, 2020. (https://www.hipaajournal.com/small-and-medium-sized-healthcare-providers-most-likely-to-be-attacked-with-ransomware)
[27] Ron Southwick, "After Cyberattack and Other Financial Woes, an Illinois Hospital Closes its Doors," *Chief Healthcare Executive,* June 20, 2023. (https://www.chiefhealthcareexecutive.com/view/after-cyberattack-and-other-financial-woes-an-illinois-hospital-closes-its-doors)
[28] Ibid.

Each of these efforts aims to support greater cyber resilience in the health care sector. Rather than create another set of guidelines, CMS can use its position to amplify many of these resources to encourage stakeholders to prioritize implementation. Where CMS can add unique guidance is on the issue of the security of operational technology and medical Internet of Things devices where continued operation of the device may trump concerns about the confidentiality of the data.

CMS also has a unique opportunity to build on incentivization programs that support advancement in cybersecurity resilience preparation.

CMS should leverage its unique capabilities to focus on overall operational resilience to supplement rather than duplicate existing guidelines, regulations, and resources.

1. **Leverage Conditions of Participation and Conditions for Coverage to elevate baseline cybersecurity preparedness requirements.**

   Care centers that participate in Medicare and Medicaid programs are required to meet conditions established by CMS through their Conditions of Participation and Conditions for Coverage.[29] CMS should amend these requirements to include the implementation of basic cybersecurity guidance provided in the Healthcare and Public Health Cybersecurity Performance Goals. CMS should also require demonstrated efforts by providers to educate their workforce on cyber threats and response. To support this, CMS should promote workforce training materials provided by CISA, HHS, and the Health Sector Coordinating Council Cybersecurity Working Group.[30] CMS should identify existing or needed financial incentives and grant programs to help providers implement the performance goals without imposing a burden on under-resourced hospitals, particularly Critical Access Hospitals.

2. **Build on existing incentivization programs to encourage greater prioritization of cybersecurity for operability.**

   CMS can expand on the existing Quality Payment Program, particularly the Merit-based Incentive Payment System (MIPS) track, to include cyber-related performance goals. There may be existing performance categories like improvement activities or promoting interoperability that provide a viable framework for including cyber-related goals. If existing categories are insufficient, CMS should consider a new category. CMS should

[29] "Conditions for Coverage (CfCs) & Conditions of Participation (CoPs)," *Centers for Medicare & Medicaid Services,* accessed June 11, 2026. (https://www.cms.gov/medicare/health-safety-standards/conditions-coverage-participation)

[30] "Healthcare and Public Health Sector: Strengthen your Defenses and Mature your Cybersecurity Efforts," *Cybersecurity and Infrastructure Security Agency*, accessed June 11, 2026. (https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare/mature-your-cybersecurity-efforts); "Cyber Resource Library," *Department of Health and Human Services Cyber*, accessed June 11, 2026. (https://hhscyber.hhs.gov/resources.html); "HSCC Cybersecurity Training Video Series," *Health Sector Coordinating Council Cybersecurity Working Group*, April 2023. (https://healthsectorcouncil.org/hscc-cybersecurity-training-video-series)

leverage this program to have health care providers report on cyber workforce training efforts and attest to basic cyber practices under the cybersecurity performance goals.

3. **Inform HHS efforts to identify systemically important entities and workforce gaps.**

   CMS should support HHS efforts as a sector risk management agency — particularly the efforts of ASPR's Office of Critical Infrastructure Protection — by leveraging information from Medicare and Medicaid programs. For example, to aid efforts to identify systemically important entities as defined in National Security Memorandum 22, CMS should identify entities like Change Healthcare that process significant shares of Medicare and Medicaid claims or provide services to many Medicare and Medicaid hospitals. Including such entities in HHS's systemically important entities list will enable appropriate oversight, planning, and preparedness. Additionally, given the capacity of technology to act as a force multiplier, CMS should encourage HHS to treat the health care cybersecurity workforce gap as a priority comparable to the clinical workforce shortages that have long attracted federal attention.

Conclusion

The cyber health of the nation's hospitals has a very real effect on the quality of care that Americans receive at hospitals and clinics across the country. CMS has a unique and vital role to play in fostering a more resilient sector that not only protects personal health information but can survive and operate through a cyber crisis.

Thank you for considering our comments. We look forward to seeing how our input is incorporated into your ongoing policy work to secure this most vital of critical infrastructure sectors.