HEALTHCARE LEADERSHIP COUNCIL

MEMBERSHIP MEETING

January 24, 2018

Transforming Healthcare Through Innovation and Collaboration: Confidentiality and Security

State of Play: *On December 5, the National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce published the second draft of the proposed update to the Framework for Improving Critical Infrastructure Cybersecurity. The second draft update aims to clarify, refine and enhance the Cybersecurity Framework, amplifying its value and making it easier to use. According to NIST, the Framework enables organizations to apply the principles and best practices of risk management to improving security and resilience. It provides a "common organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today." The latest draft reflects comments received to date, including those from a public review process launched in January 2017 and a workshop in May.*

HLC Position: *HLC leads a broad group of organizations, collectively known as the Confidentiality Coalition, to ensure that policymakers strike the right balance between the protection of confidential health information and the information-sharing needed to provide the very best quality of care. The coalition is active with Congress and the administration on policies related to data exchange, privacy, data security, and cybersecurity. Members believe that regulatory clarity is key to securing health information flow and support efforts to create a uniform national privacy standard, based on the Health Insurance Portability and Accountability Act's (HIPAA) privacy rule, rather than the inconsistent and conflicting state laws that currently supersede federal regulation.*

HLC Recent Activity:

- Throughout the fall, HLC through the Confidentiality Coalition has worked with congressional staff and industry on legislative language that would provide incentives to uphold preeminent security practices to ensure cyberreadiness for the healthcare industry.
- As part of the annual Health Datapalooza conference planning, HLC was selected by Academy Health to review conference applications for privacy and cybersecurity speakers and panel presentations.
- HLC continues to work with a coalition of stakeholders committed to aligning federal confidentiality regulations for substance abuse (42 CFR Part 2) with HIPAA to allow appropriate access to patient information that is essential for providing comprehensive care. Currently patient records from alcohol and drug abuse programs are prohibited from being shared for purposes of treatment, payment, or healthcare operations without written consent. The group advocates with Congress and the administration in support of the "Legacy Act" (S. 1850) and the "Overdose Prevention and Patient Safety (OPPS) Act" (H.R. 3545), which would apply HIPAA standards to a patient's entire medical record, including addiction records, to ensure that providers and organizations have the information necessary for safe, effective treatment and care coordination.

- On October 4, HLC attended the U.S. Chamber of Commerce Annual Cybersecurity Summit, where participants discussed the current state of cyber threats for all industries, including healthcare. The U.S. Chamber of Commerce subsequently followed up with HLC staff to explore collaborative efforts related to healthcare and cybersecurity threats.
- In October, the executive director of the National Health Information Sharing and Analysis Center (NH-ISAC) Healthcare and Public Health Sector Coordinating Council (Departments of Homeland Security and Health and Human Services (DHS/HHS) public private partnership) met with HLC staff to understand the interplay of the various sectors in the healthcare industry to inform the policy work of the NH-ISAC on cybersecurity matters.
- On September 28, the Confidentiality Coalition met with Office of Civil Rights (OCR) Director Roger Severino, to encourage further modifications to the HHS Breach Reporting Tool website – particularly, to indicate whether a breach of protected health information is due to a cyberattack against an organization, as well as to encourage OCR to remove organizations from the website upon resolution of the breach.
- On July 27, the Confidentiality Coalition was joined by a representative from OCR to discuss recent actions taken to update the HIPAA Breach Reporting Tool website. Coalition members provided feedback on additional changes to the site to improve information uploading or input processes.
- On July 24, the Confidentiality Coalition wrote HHS about planned improvements to the HIPAA Breach Reporting Tool. In its comments, the coalition supported administration efforts to revisit this reporting tool for breaches of 500 or more individuals, which was required by the HITECH Act. The coalition recommended that the administration maintain efforts to notify consumers, work more closely and cooperatively with industry, seek to differentiate between victims of cyberattacks and organizations with inadequate security practices, and create a mechanism for HHS to remove organizations from the website once security issues have been rectified.
- On June 15, the Confidentiality Coalition held its annual “HIPAA 101” Hill briefing. Experts from New York-Presbyterian Hospital and McKesson Corporation explained the HIPAA privacy and security rules to congressional staffers and answered questions.
- On June 8, the Confidentiality Coalition met with the Office of the National Coordinator (ONC) Office of the Chief Scientist to discuss the Precision Medicine Initiative and the federal government’s efforts to protect patient privacy while sharing important research data.
- On June 8, the Confidentiality Coalition submitted comments to the Energy and Commerce Subcommittee on Oversight in connection to its hearing, “Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity.” The Confidentiality Coalition emphasized the importance of cyber information-sharing tools and applauded the cooperative nature of HHS’s plans to create a single cybersecurity point of contact for healthcare organizations. The coalition also successfully encouraged members of Congress to inquire about reforms to the HIPAA Breach Reporting Tool website, also known as the breach “wall of shame.” The coalition urged HHS to differentiate between organizations that use appropriate security practices and were simply unfortunate victims of cyberattacks and those who have not taken appropriate action in cybersecurity.
- HLC continues to work to resolve the patient matching dilemma created by the congressional ban on a unique patient identifier. HLC has encouraged Congress to allow HHS to provide technical assistance to private-sector initiatives promoting patient safety by correctly matching patients with their health information.

    - A provision included in the House Committee on Appropriations' FY 2018 proposed budget directs HHS to complete a report on how patient matching would improve care, reduce costs, and decrease errors. It also directs the department to investigate what patient safety improvements hospitals may experience if participation in a patient-matching system became a requirement for the Medicare program. In a separate section, it encourages ONC to engage with stakeholders on private-sector-led initiatives to develop a coordinated strategy that will promote patient safety by accurately identifying patients with their health information.
    - On April 4, HLC and other organizations wrote House and Senate Appropriations Committee leaders, encouraging them to include key language in the FY 2018 Labor-HHS appropriations bill explicitly allowing HHS to provide technical assistance to private-sector initiatives promoting patient safety by correctly matching patients with their health information. Similar language was included in a 2017 draft bill, but was not included in the continuing resolution that funded the government.
- On June 2, the Health Care Industry Cybersecurity Task Force created by the Cybersecurity Information Sharing Act (CISA) in December 2015 reported back to Congress. The task force spent the last year receiving input from experts in and out of the healthcare industry and the public in order to develop the report. Recommendations include revising Anti-Kickback laws to allow organizations to share cyber resources; phase out old, insecure technologies; build better cybersecurity protections into medical devices through FDA regulations or guidance; better assure the authenticity of workers, patients, devices, and electronic health records (EHRs); think about small- and medium-sized providers who cannot afford technical resources; establish and implement good "cybersecurity hygiene" across healthcare; develop educational resources; and ensure the protection of large data sets. Statutory authority for the task force has expired now that its recommendations have been made to Congress.
    - The Confidentiality Coalition provided policy advice in the creation of this task force. Several HLC and coalition members participated as members of the task force.
- On May 25, Confidentiality Coalition members were joined by leaders from the Office of the Chief Information Security Officer at HHS. During this meeting, HHS officials discussed the department's public-facing role to assist health organizations in resisting cyberattacks. It aims to be the single point of contact at HHS for cybersecurity.
- On April 27, HLC moderated a panel at the annual Health Datapalooza conference, titled "Getting Privacy and Security Right from the Start(up)." Experts from OCR, the Federal Trade Commission (FTC), QuintilesIMS, and HLC spoke about educating entrepreneurs on how to protect health information and share it with consumers.
- HLC and the Confidentiality Coalition continue to monitor increasing FTC and Federal Communications Commission (FCC) involvement in healthcare, particularly regarding data breaches and non-HIPAA data.
- The Confidentiality Coalition continues to monitor the environment for healthcare organizations under the Telephone Consumer Protection Act (TCPA). Members believe that the TCPA should provide greater flexibility and regulatory clarity for healthcare organizations to communicate important health information by phone to consumers.
- HLC discussed health information flow and confidentiality issues at in-district meetings with incoming and returning members of the 115th Congress. These meetings educated incoming members of the 115th Congress about this issue and have allowed us to continue being a resource for those members.

Key Action Since the September 2017 Membership Meeting:

- On January 2, 2018, the Substance Abuse and Mental Health Services Administration published a final rule to provide greater flexibility in disclosing patient identification information while protecting confidentiality of substance use disorder patient records.
- On December 18, the HHS Office for Civil Rights (OCR) launched an array of new tools and initiatives in response to the opioid crisis, while implementing the 21st Century Cures Act. Highlights of these actions include:
    - Two new HIPAA webpages focused on information related to mental and behavioral health, one for professionals and another for consumers;
    - New HIPAA guidance on sharing information related to mental health and substance use disorder treatment;
    - New collaboration with partner agencies within HHS to identify and develop model programs and materials for training healthcare providers, patients, and their families regarding permitted uses and disclosures of Personal Health Information (PHI);
    - Updated guidance on HIPAA and research, as called for in the Cures Act;
    - Launch of a working group to study and report on the uses and disclosures under HIPAA of PHI for research purposes.
- On November 16, House Energy and Commerce Committee Chairman Greg Walden (R-OR) sent a letter to HHS asking the department to secure the cybersecurity of medical devices by shoring up supply chains. The letter asks that HHS begin requiring device manufacturers to list bills of materials; an accounting of third-party software components used in each product. The letter asks HHS to develop a plan to coordinate stakeholders in medical devices to form a framework to encouraging bills of materials by December 15.
- On November 1, House Energy and Commerce Committee members Representatives Billy Long (R-MO) and Doris Matsui (D-CA) introduced H.R. 4191, the "HHS Cybersecurity Modernization Act," legislation to address cyber threats to HHS.
- On October 27, Chairman Greg Walden (R-OR) published an op-ed, entitled "Consumer Protection in the 21st Century," raising questions surrounding business practices by tech companies and their impact on consumers. The op-ed also announces a series of hearings the committee will hold in November to examine how actions taken by online businesses affect consumers' privacy and choices without their knowledge.
- On October 26, Representative Markwayne Mullin (R-OK) asked for unanimous consent on the House floor to become the lead Republican sponsor of the "Overdose Prevention and Patient Safety (OPPS) Act," H.R. 3545. According to the bill's sponsors, H.R. 3545 would modernize addiction treatment by ensuring providers have access to their patients' entire medical history. Currently, information about patients' addiction treatment is prohibited from being shared with providers.
- On October 10, the ONC announced a secure API server showdown challenge, urging stakeholders to focus on health IT security in building Fast Healthcare Interoperability Resources (FHIR) servers. The challenge will ideally identify unknown security vulnerabilities in the way open source FHIR servers are implemented.
- On September 13-14, the National Committee on Vital Health and Statistics (NCVHS) met to discuss health information privacy and security beyond HIPAA. As follow-up to that meeting, NCVHS has collected information to develop a report on the privacy and security landscape for health information in the United States that extends beyond the HIPAA privacy and security rules.