2012 Privacy Activity and Confidentiality Coalition Accomplishments

Issue: *Since April 2003, healthcare providers, plans, and clearinghouses have been subject to the Health Insurance Portability and Accountability Act (HIPAA) privacy standards, which govern the use and disclosure of protected health information. These regulations protect the privacy of a patient's medical information and ensure that necessary information is available for providing quality healthcare and conducting vital medical research. HHS continues to promulgate rules to implement the health information technology (HIT) provisions of the American Recovery and Reinvestment Act of 2009 (ARRA, P.L. 111-5). In addition to many provisions aimed at creating a national HIT infrastructure, ARRA also created new federal rules governing the privacy and security of health information. As more health information is transmitted electronically, state and federal governments have become more involved in regulating the exchange of health information.*

Confidentiality Coalition Position: *The Confidentiality Coalition advocates for policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions. The Confidentiality Coalition believes that the varying state standards allowed by the HIPAA Privacy Rule impede the sharing of information in the context of a national health information network. In order for interoperability to be achieved, Congress should make the HIPAA Privacy Rule the uniform national standard, replacing the conflicting patchwork of state privacy laws.*

Confidentiality Coalition Accomplishments in 2012:

- The Confidentiality Coalition works closely with key legislators and regulators to ensure that privacy legislation and regulation do not impede efforts to provide safe, high-quality, and coordinated healthcare.
- HLC met with PCORI Executive Director Joe Selby, M.D., in early December to discuss the creation of national research databases and the need for data exchange to improve health outcomes for individuals and populations.
- In October, the Confidentiality Coalition hosted the CEO of the Genetic Alliance to discuss the importance of sharing clinical data for research.
- In October, the Confidentiality Coalition met with congressional staff to discuss health research legislation.
- In September, the Confidentiality Coalition hosted staff from the Commerce Department to discuss its privacy multi-stakeholder process regarding mobile application transparency.

- The Confidentiality Coalition continues to monitor cybersecurity legislation and meet with congressional staff as appropriate regarding the need to remove HIPAA-covered entities and business associates from duplicative regulation by the Federal Trade Commission (FTC) and other non-HHS agencies.
    - On July 30, the Confidentiality Coalition sent a letter to Senate majority and minority leaders, as well as staff on the Senate Judiciary, Commerce, and Health, Education, Labor, and Pensions (HELP) Committees to express opposition to any amendments to the "Cybersecurity Act of 2012" (S. 3414) that would alter HIPAA or HITECH, either directly or indirectly.
    - In conjunction with the letter, the Confidentiality Coalition met with Senate Commerce and Judiciary Committee staff to advocate support of a clean cybersecurity bill with no health privacy amendments.
- In June, the Confidentiality Coalition held a two-part Capitol Hill briefing series on the health privacy landscape.
    - On June 25, the Confidentiality Coalition held a briefing for over 50 congressional staffers on the value of health information exchange. Speakers discussed how electronic health data is being exchanged to improve patient care and health outcomes, while maintaining patient privacy.
    - On June 4, the Confidentiality Coalition held a briefing for nearly 35 congressional staffers on HIPAA in the 21st Century. A panel discussed how health information is protected across a variety of care settings.
- The Confidentiality Coalition has begun tracking federal privacy policy as related to wireless devices and mobile health (m-health) applications.
- In June, the Confidentiality Coalition submitted comments on the governance structure for the Nationwide Health Information Network (NwHIN), a national HIT infrastructure meant to facilitate data exchange among healthcare providers.
- In May, the Confidentiality Coalition launched a new website. The website highlights legislative and regulatory developments in health privacy policy, as well as the Coalition's ongoing activities.
- On May 7, the Confidentiality Coalition submitted comments to HHS on the notice of proposed rulemaking delineating standards and criteria for the certification of EHRs under stage 2 of the meaningful use program.
- On March 21, the Confidentiality Coalition submitted comments in response to an "information collection request" regarding the Office of the National Coordinator for Health Information Technology's (ONC) proposed Privacy and Security Consumer Attitudes Survey.

Regulatory Action in 2012:

Office for Civil Rights (OCR)

- On October 11, OCR Director Leon Rodriguez spoke at the HIPAA West Summit, stating the department will continue its HIPAA enforcement effort, and will also make permanent a pilot project that conducts audits of covered entities for compliance with HIPAA privacy and security rules and breach notification standards. Rodriguez also stated that he has no new information about the forthcoming final HIPAA "omnibus" rule.
    - The Office of Management and Budget (OMB) is still reviewing the omnibus rule, which will include the final breach notification rule required by the

HITECH Act, the final HIPAA enforcement rule, the final rule implementing HIPAA privacy and security changes mandated in HITECH, and a final rule implementing HIPAA changes mandated in the Genetic Information Nondiscrimination Act (GINA).

- On September 17, HHS announced a settlement with Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. (MEEI) for potential violations of the HIPAA Security Rule. MEEI will pay HHS $1.5 million and will also take corrective action to improve policies and procedures to safeguard the privacy and security of its patients' protected health information.
- On June 26, OCR posted on its website the protocol used to conduct audits of covered entities for compliance with HIPAA privacy and security rules and breach notification standards. The HIPAA Audit Program was funded by the HITECH Act. OCR anticipates that it will audit approximately 150 covered entities through December 2012.
- On June 26, the Alaska Department of Health and Social Services agreed to pay HHS $1,700,000 to settle possible violations of the HIPAA Security Rule, in addition to agreeing to take corrective action to safeguard properly the electronic protected health information of Alaska Medicaid beneficiaries.
- On May 31, OCR Director Leon Rodriguez released a "right to access" memorandum educating patients about their rights to access their medical records under the HIPAA Privacy Rule. The memo detailed available OCR tools and resources to educate consumers regarding their rights to see and obtain a copy of their medical records.
- On April 17, OCR announced that Phoenix Cardiac Surgery has agreed to pay HHS a $100,000 settlement and take corrective action to implement policies and procedures to safeguard patients' protected health information.
- On March 26, officials from OCR announced that the long-awaited final HIPAA "omnibus" rule was sent to the Office of Management and Budget (OMB), signaling the rule will be released publicly in the near future. The omnibus rule will include the final breach notification rule required by the HITECH Act, the final HIPAA enforcement rule, the final rule implementing HIPAA privacy and security changes mandated in HITECH, and a final rule implementing HIPAA changes mandated in the Genetic Information Nondiscrimination Act (GINA).
    - In late June, OMB extended its review of the final HIPAA "omnibus" rule. The final rule has yet to be published.
- In 2012, OCR began auditing covered entities for compliance with HIPAA privacy and security rules and breach notification standards under the HIPAA Audit Program funded by the HITECH Act. OCR anticipates that it will audit approximately 150 covered entities through December 2012.

Office of the National Coordinator for Health IT (ONC)

- At the September HIT Policy Committee meeting, National Coordinator for HIT Dr. Farzad Mostashari announced that ONC is no longer pursuing a regulatory approach to establish a governance structure for the Nationwide Health Information Network (NwHIN). The policy shift came in response to comments to the request for information issued by the department in May on the creation of a governance structure, which expressed concern that regulation could hinder electronic health information exchange. ONC will continue to monitor exchange activities and provide

guidance on best practices, and may decide to renew a regulatory approach in the future.
    - In October, ONC announced it was nearly finished transferring operational responsibilities for the NwHIN Exchange to a new public-private organization called Healtheway. Healtheway now is the business arm of NwHIN Exchange, which has been renamed the eHealth Exchange.
- In September, ONC officials launched a video game offering privacy and security training for healthcare providers. The video game will be available at no cost, and is geared towards small medical practices.
- In September, HHS and the U.S. Veterans Affairs Department demonstrated the successful use of "metadata" standards to tag and segment clinical patient information based on its sensitivity. Metadata – which refers to elements that describe data – are considered to be a necessary step in the process of developing a more robust health information exchange.
    - The demonstration was conducted as part of the ONC Data Segmentation Initiative, which is developing standards to allow providers to share specified portions of an electronic medical record, while keeping certain information separate. The technology could potentially be used to give patients choice over what health information is shared by providers electronically.
- On August 23, ONC and CMS released final rules governing stage 2 of the electronic health record (EHR) "meaningful use" incentive program.
    - The ONC final standards and certification rule delineates standards and criteria for the certification of EHRs under stage 2 of the meaningful use program. The rule streamlines the certification process and revises the definition of certified EHR technology to let providers adopt only the technology necessary to meet the specific stage of meaningful use they are seeking to achieve.
    - The final rule clarified that accounting of disclosures functionality in EHRs will remain optional for stage 2. ONC until wait for HHS Office of Civil Rights (OCR) to release a final accounting of disclosures rule, in order to consider how best to align EHR certification criterion with provisions in the final OCR rule.
    - The CMS final rule outlines criteria for hospitals and healthcare providers seeking to attest to stage 2 of the meaningful use program. Privacy- and security-related requirements that were adopted in the final rule include a security risk assessment, as well as addressing encryption of data not currently being transmitted.
- On May 15, ONC published a "request for information" (RFI) in the Federal Register on the creation of a governance structure for the Nationwide Health Information Network (NwHIN), a national HIT infrastructure meant to facilitate data exchange among healthcare providers. The governance mechanism will include rules on privacy and security requirements to establish a common trust framework for the exchange, as well as on other technical and business practice requirements. Comments were due June 14.
- In May, ONC's Office of the Chief Privacy Officer released a "Guide to Privacy and Security of Health Information," an instructional guide designed to help healthcare practitioners, staff, and other professionals better understand the important role privacy and security play in electronic health information exchange.
- On March 22, ONC released guidance on privacy and security for states building health information exchanges (HIE) under ONC's Cooperative Agreement Program.

The guidance offers a set of recommendations for privacy and security policies and procedures to build public trust and establish a consistent approach for states.

- On March 16, ONC held the Mobile Devices Roundtable: Safeguarding Health Information. The purpose of the roundtable was to gather public, industry, and subject matter experts' input that will help inform the development of an effective and practical way to bring awareness and understanding to those in the clinical sector about securing and protecting health information when using mobile devices.
- In March, ONC announced it was seeking public input on privacy and security issues and best practices related to the use of mobile devices by providers and other healthcare delivery professionals to gain access to, store, and transmit health information. Comments were accepted until March 30.
- On February 21, HHS republished an information collection request in the Federal Register regarding its intent to conduct a consumer survey of attitudes toward the privacy and security aspects of EHRs and electronic health information exchange.

Federal Trade Commission (FTC)

- On March 26, the FTC released its final report on consumer privacy, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers."
  - The FTC will host a workshop on May 30 to address mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers.

Legislative Action in 2012

- On December 3, Representative Mike Honda (D-CA) introduced the Health Care Innovation and the Marketplace Technologies Act of 2012. Among other things, the bill would establish the "Office of Wireless Health Technology" within the Office of the Commissioner at FDA that would provide recommendations to improve practices with regard to wireless health technology and align such practices with the practices of other Federal agencies without compromising patient safety or privacy.
- On October 11, Republican members in both the U.S. House of Representatives and Senate sent President Obama a letter urging him to refrain from issuing an executive order related to cybersecurity. The lawmakers argue than an executive order would threaten freedom of expression online; they encouraged a diversity of public and private sector approaches.
  - In early September, the White House circulated a draft executive order aimed at protecting national infrastructure from cyber attacks.
  - On August 2, the "Cybersecurity Act of 2012" (S. 3414) was set aside in the Senate, eight votes short of the 60 necessary to end debate on the bill and bring it to a vote. Partisan division was heightened by non-germane amendments offered, such as repeal of PPACA. It is possible that the Senate will resume the cybersecurity debate during the upcoming "lame duck" session in Congress.
  - The House of Representatives declared the week of April 23 as "Cybersecurity Week."
  - In February, a group of Senate committee leaders introduced bipartisan legislation to secure the cyber systems of the nation's essential services. The

"Cybersecurity Act of 2012" (S. 2105) was introduced by Senators Joe Lieberman (I-CT), Susan Collins (R-ME), Jay Rockefeller (D-WV), and Dianne Feinstein (D-CA).
    - On February 16, the Senate Committee on Homeland Security and Governmental Affairs held a hearing on S. 2105.
- On June 27, Senator Franken introduced the "Protect Our Health Privacy Act" (S. 3351), which would require encryption of data stored on portable media devices and also extend "minimum necessary" requirements to HIPAA business associates.
- On June 21, Senator Pat Toomey (R-PA) introduced the "Data Security and Breach Notification Act of 2012" (S. 3333). The bill would require entities that collect and maintain personal information of individuals to secure that information and provide notice in the case of a breach of security.
- On May 30, the Senate Health, Education, Labor, and Pensions (HELP) Committee held a field hearing in Minnesota on "Ensuring Patients' Access to Care and Privacy: Are Federal Laws Protecting Patients?"

Other Health Privacy Activity in 2012

- On October 11, the Presidential Commission for the Study of Bioethical Issues released a report calling for comprehensive policies and laws to protect the privacy and security of individuals' genomic data. In the report, the Commission offers recommendations for how to reconcile the need for protecting privacy with the need for gathering data from many individuals to advance discoveries with genome sequencing.
- On October 9, the HHS Office of the Inspector General (OIG) released a report titled, "CMS Response to Breaches and Medical Identity Theft." The OIG found CMS could take steps to better respond to breaches of Medicare beneficiaries' protected health information. For the report, OIG studied CMS breaches that occurred between September 23, 2009 – when the HHS breach notification rule took effect – and December 31, 2011.
- In September, GAO released a report, "FDA Should Expand Its Consideration of Information Security for Certain Types of Devices," recommending that FDA develop and implement a plan expanding its focus on information security risks for complex medical devices such as insulin pumps and implantable defibrillators.
- On August 1, the Government Accountability Office (GAO) released a report on federal privacy laws. GAO was asked to examine the impact of recent technology developments on existing federal privacy laws and identify actions federal agencies can take to protect against and respond to breaches of personal information. GAO found that existing federal data privacy protection laws are ineffective and should be revised better to reflect the changing technology landscape.
- On July 11, the National Institute of Standards and Technology (NIST) released a proposed update to its guidelines for securing mobile devices used by the federal government. The Guidelines for Managing and Securing Mobile Devices in the Enterprise, a revision to the Guidelines on Cell Phone and PDA Security, was drafted to reflect today's technology and focuses on smart phones and tablets. NIST accepted comments until August 17.

- On July 11, the Health Information Trust Alliance (HITRUST) announced the formation of the HITRUST De-Identification Working Group to propose standards for health de-identification and the appropriate use and handling of de-identified data as defined by the HIPAA Privacy Rule.
    - OCR is expected to issue guidance on implementing requirements for the de-identification of protected health information per the HITECH Act.
- On June 5 and 6, the Health Datapalooza was held in Washington, D.C., organized by the Health Data Initiative (HDI) Forum.
    - At Datapalooza, CMS formally launched the Office of Information Products and Data Analysis (OIPDA), a new office dedicated to the management, use, and dissemination of health data – with a focus on patient privacy. OIPDA will make the development, management, use, and dissemination of data and information a core function of CMS.