



## 2011 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. The Department of Health and Human Services (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 deeply involved in regulating the exchange of health information.*

**HLC Position:** *The Confidentiality Coalition advocates for policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enable 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.*

### Regulatory Action in 2011:

- On November 8, the Office for Civil Rights (OCR) announced a pilot program to perform up to 150 audits of covered entities to assess privacy and security compliance. Audits conducted during the pilot phase will begin in November 2011 and conclude by December 2012.
- On November 3, HHS published 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 electronic health records (EHRs) and electronic health information exchange.

- In a November 1 Federal Register notice, HHS proposed to conduct a nationwide communications campaign to meet the congressional mandate to educate the public about privacy and security of electronically exchanged personal health information.
- On October 20, HHS Secretary Kathleen Sebelius announced that the Office of the National Coordinator for Health Information Technology (ONC) created a new senior position of principal deputy to manage more effectively the office's efforts to drive meaningful use of electronic health records and health information exchanges.
- On October 5, ONC launched its Data Segmentation Initiative. The goal of the program is to produce a pilot project that will allow providers to share specified portions of an electronic medical record, while keeping certain information separate.
- HHS held a Consumer Health IT Summit on September 12. At the summit, Secretary Sebelius announced the appointment of Leon Rodriguez as the new OCR director.
- On September 12, Secretary Sebelius announced new proposed rules issued jointly by HHS, the Centers for Medicare and Medicaid Services (CMS), and the Centers for Disease Control and Prevention (CDC) designed to improve consumer access to laboratory testing results.
- On September 12, federal officials announced a voluntary Personal Health Record (PHR) Model Privacy Notice to provide a standardized template to help consumers compare and make decisions about PHR products based on their data practices, as well as privacy and security policies.
- ONC released the final Federal Health IT Strategic Plan for 2011 through 2015 in September. In response to issues raised in the public comments, the final strategic plan calls for establishing an HHS interdivision task force to develop an updated approach to certain HIT privacy and security issues.
- On September 1, OCR released two reports detailing HHS's enforcement of the HIPAA privacy and security rules, as well as information about data breaches reported to the agency. This was HHS's first report, which is required by ARRA.
- On September 6, ONC launched its Query Health Initiative to establish standards for requesting population health data from widely distributed sources, including EHRs.
- On July 22, HHS announced plans to update regulations protecting human research subjects. The agency later announced it was extending the comment deadline one month and accepted public comment on the advance notice of proposed rulemaking through October 26.
- ONC is on schedule to release both a proposed and final rule for Stage 2 of the "meaningful use" electronic health record (EHR) incentive program in 2012.
  - Over the summer, the HIT Policy Committee approved a recommendation to delay the transition from Stage 1 to Stage 2 by one year for providers attesting to Stage 1 this year.
- In August, the HHS Privacy & Security Tiger Team offered recommendations to the Office of the National Coordinator's (ONC) HIT Policy Committee regarding the privacy and security implications of a patient's ability to view and download his or her electronic health information.
- On July 22, HHS announced plans to update regulations protecting human research subjects. The agency accepted public comment on the advance notice of proposed rulemaking through September 23.
- In July, the HIT Policy Committee accepted recommendations from the Privacy & Security Tiger Team regarding amendments and corrections to patient medical records.

- On July 6, National Coordinator for Health Information Technology (HIT) Farzad Mostashari announced his support for the HIT Policy Committee's recommendation to delay by one year Stage 2 of the meaningful use electronic health record (EHR) incentive program for healthcare providers attesting to meeting Stage 1 criteria this year.
  - At its June meeting, the HIT Policy Committee approved the meaningful use work group's revised Stage 2 objectives and criteria and the recommendation to delay the transition from Stage 1 to Stage 2 by one year.
- Also on July 6, HHS entered into a resolution agreement with the University of California at Los Angeles Health System (UCLAHS) to settle potential violations of the HIPAA Privacy and Security Rules. UCLAHS agreed to settle for \$865,500 and committed to a corrective action plan aimed at remedying gaps in its compliance with the rules. The agreement marks HHS's third largest settlement for HIPAA violations.
- On June 22, National Coordinator for HIT Mostashari indicated that ONC plans to publish a proposed rule promoting the broader use of existing metadata standards. 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.
- On June 3, CMS released a proposed rule implementing a provision from ACA requiring HHS to make available Medicare data to qualified entities for the evaluation of provider and supplier performance. Entities that meet certain qualifications will be able to access patient-protected Medicare data to produce public reports on physicians, hospitals, and other healthcare providers. The reports would combine Medicare claims data with private-sector claims data to identify high-quality, cost-effective providers.
- In June, the HIT Policy Committee accepted the Privacy & Security Tiger Team's recommendations on EHR user authentication, patient portals, and security assessments, as well as its amended recommendation related to digital certificates.
- On May 31, the HHS Office for Civil Rights (OCR) published a proposed rule governing the sharing of and access to protected health information. The HITECH Act required covered entities that use or maintain an electronic health record to provide, upon request, an accounting of disclosures made for treatment, payment, and healthcare operations purposes through an EHR over a three-year period. Comments on the proposed rule will be accepted until August 1, 2011.
  - Comments on the proposed rule were accepted until August 1, 2011. The proposed rule was widely criticized by healthcare organizations and certain consumer groups as unworkable and not providing significant privacy benefits to patients.
- On May 19, the Office of the National Coordinator for Health Information Technology (ONC) published a notice in the Federal Register requesting clearance from the Office of Management and Budget (OMB) to collect information from the general public as well as healthcare providers to inform the development and testing of communication messages and strategies around health information technology (HIT) and related privacy issues. Comments on the proposed project, the Comprehensive Communication Campaign for HITECH Act, were due to ONC June 19.
- On May 17, the HHS Office of the Inspector General (OIG) released an audit report evaluating the oversight and enforcement actions of the Centers for Medicare and Medicaid Services (CMS) with respect to the HIPAA Security Rule. OIG concluded that CMS's actions were not sufficient to ensure that hospitals and other covered

entities effectively implemented the Security Rule, and recommended that CMS implement procedures for conducting compliance reviews.

- On May 17, OIG released a second audit report assessing information technology security controls included in health information technology standards. OIG found the Office of the National Coordinator for Health Information Technology has not developed the general security controls necessary to create a secure environment for health data.
- On May 10, OCR staff reiterated publicly that a final omnibus rule strengthening HIPAA privacy and security safeguards will be released by the end of 2011.
- In May, the HHS HIT Policy Committee met to discuss the timing and requirements for Stage 2 of the Electronic Health Record (EHR) incentive program. In June, the Policy Committee plans to review recommendations from its HIT and privacy-related workgroups. Once the committee approves the recommendations, it will send them to CMS and ONC for review.
  - A Notice of Proposed Rulemaking (NPRM) on Stage 2 of meaningful use is expected in the fourth quarter of 2011.
- To help state attorneys general begin to implement their enforcement authority under the HITECH Act, the HHS Office of Civil Rights (OCR) held 2-day, instructor-led HIPAA Enforcement Training courses in four locations across the country in May and June.
- In May, OCR and the National Institute of Standards and Technology (NIST) co-hosted the 4th annual conference "Safeguarding Health Information: Building Assurance through HIPAA Security" in Washington, DC.
- On April 13, the privacy and security Tiger Team of the HHS HIT Policy Committee presented a series of recommendations on policy topics related to electronic health records (EHRs) and proposed data security requirements for the next stage of the "meaningful use" EHR Incentive Program.
- On April 8, HHS Secretary Kathleen Sebelius named Farzad Mostashari as national coordinator for health IT to replace outgoing head David Blumenthal.
- On March 31, HHS issued a proposed rule governing accountable care organizations (ACOs) participating in the Medicare Shared Savings Program. The proposed rule would require providers in an ACO to notify the beneficiary that the beneficiary's claims data may be shared with the ACO, and provide the opportunity for the beneficiary to opt out of those data sharing arrangements. Data sharing would be limited to the purposes of the Shared Savings Program and would require compliance with applicable privacy rules and regulations, including HIPAA.
- OCR has requested a \$5.6 million increase for its fiscal year 2012 budget so it can follow HIPAA enforcement and compliance requirements. The additional funds would be used to investigate data breach reports, as well as to hire "regional privacy officers" to offer HIPAA guidance and education to business associates, covered entities, and individuals.
- In February, OCR imposed its first-ever civil monetary penalty (CMP) on a covered entity for violating the HIPAA Privacy Rule, ordering Cignet Health to pay \$4.3 million.
- In a separate enforcement action, HHS also announced in February that Mass General will pay the federal government \$1 million to resolve a complaint that it violated the HIPAA Privacy Rule when an employee lost the paper medical records of 192 patients.
- On February 4, the FTC released a frequently-asked-questions guide to medical identity theft for healthcare providers and insurers.

- On January 21, the FTC announced it was extending the deadline for the public to comment on a preliminary staff report issued on December 1, 2010, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policy Makers." The commission extended the original January 31 deadline until February 18 to encourage participation by all stakeholders.

### **Legislative Action in 2011:**

- On November 9, the Senate Committee on the Judiciary held a hearing of the Subcommittee on Privacy, Technology and the Law entitled, "Your Health and Your Privacy: Protecting Health Information in a Digital World."
- On September 8, Senator Richard Blumenthal (D-CT) introduced the "Personal Data Protection and Breach Accountability Act of 2011" (S. 1535) to protect citizens' personal information from online data breaches.
- On September 6, House Energy and Commerce Chairman Fred Upton (R-MI) said privacy and data security would be among the panel's top priorities for the fall congressional session. Specifically, the Commerce, Manufacturing and Trade subcommittee would focus on consumer knowledge and control over online data collection.
- On July 29, Senators Herb Kohl (D-WI) and Amy Klobuchar (D-MN) sent a letter to HHS Secretary Kathleen Sebelius regarding proposed changes to the accounting of disclosures provisions in the HIPAA privacy rule.
  - They specifically addressed the utility and feasibility of creating a new consumer "right" to receive a health information access report from healthcare providers. The senators urged the secretary to direct the Office for Civil Rights (OCR) to engage stakeholders to achieve a more workable solution for implementing this new access report right.
- On July 18, Congresswoman Mary Bono Mack (R-CA) introduced the "SAFE Data Act" (H.R. 2577). The legislation would establish national notification standards for firms that experience data breaches that compromise customers' personal information.
- On June 29, the Senate Commerce, Science, and Transportation Committee held a full committee hearing on "Privacy and Data Security: Protecting Consumers in the Modern World." The hearing examined how entities, including healthcare organizations, collect, maintain, secure, and use personal information. It was the third hearing on consumer privacy held by the Commerce Committee since the beginning of the 112th Congress.
- June 15, Senator Mark Pryor (D-AR) introduced the "Data Security and Breach Notification Act of 2011" (S. 1207). The legislation would require security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach.
- On April 13, Representative Cliff Stearns (R-FL) introduced the Privacy Protection Act of 2011 (H.R. 1528), which would require entities subject to the legislation to provide consumers in clear and easy-to-understand language what information is being collected during online activity and how the information is being used. The bill is cosponsored by Representative Jim Matheson (D-UT).
- On April 12, Senators John Kerry (D-MA) and John McCain (R-AZ) introduced a Commercial Privacy Bill of Rights (S. 799) that would establish a baseline code of

conduct for how personally identifiable information and information that can uniquely identify an individual or networked device are used, stored, and distributed.

- On March 16, the Senate Commerce Committee held a hearing on “The State of Online Consumer Privacy.” The hearing kicked off the 112th Congress’s deliberations on consumer privacy, an issue that is front and center on the Commerce Committee’s agenda, and a top priority for Chairman Jay Rockefeller (D-WV).
- On February 11, Representative Jackie Speier (D-CA) offered H.R. 654, the “Do Not Track Me Online Act,” which directs the Federal Trade Commission (FTC) to prescribe regulations regarding the collection and use of information obtained by tracking the Internet activity of an individual. The bill has 10 cosponsors and was referred to the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade.
- On February 10, Representative Bobby Rush (D-IL) introduced the BEST PRACTICES Act (H.R. 611). The legislation would set ground rules and privacy minimums to assist consumers in protecting personal information with particular emphasis on online activity.
- Early this year, the Senate Judiciary Committee announced the creation of a new subcommittee on privacy, technology and the law. Senator Al Franken (D-MN) will chair and Senator Tom Coburn (R-OK) was named ranking member.

#### **Other Privacy Activity in 2011**

- On June 23, the U.S. Supreme Court struck down a Vermont law that barred the commercial use of de-identified patient data that is part of a physician’s prescribing history.
- On June 9, the Institute of Medicine (IOM) and HHS hosted the Health Data Initiative Forum to accelerate momentum for the public use of data and innovation to improve health.
- In January, the Supreme Court granted review of Sorrell v. IMS Health Inc. to decide the constitutionality of a Vermont law that bans the commercial use of de-identified patient data that is part of a physician’s prescribing history.

#### **Confidentiality Coalition Accomplishments in 2011:**

- The Confidentiality Coalition, has worked closely with key legislators and regulators to ensure privacy legislation and regulation do not impede efforts to provide safe, high-quality, and coordinated healthcare.
- The Confidentiality Coalition sent a letter to new OCR Director Leon Rodriguez welcoming him in his new position, and reiterating the Coalition’s concerns with the accounting of disclosures NPRM.
- The Confidentiality Coalition was invited by the Center for Democracy and Technology to participate in a select meeting of consumer and industry stakeholders to discuss policy related to the de-identification of healthcare information.
- The Confidentiality Coalition submitted comments on the research advanced notice of proposed rulemaking.
- In September, the Confidentiality Coalition hosted a briefing for Senate republican staff on committees of jurisdiction on accounting of disclosures.

- The Confidentiality Coalition hosted staff from the Office of the National Coordinator for Health Information Technology to discuss the office's Data Segmentation and Query Health Initiatives.
- The Confidentiality Coalition submitted comments on the accounting of disclosures proposed rule, urging the department to eliminate the access report provision and reengage stakeholders on this issue.
- The Confidentiality Coalition undertook a large advocacy campaign on Capitol Hill to educate lawmakers about the inherent problems with the accounting of disclosures NPRM.
  - The Confidentiality Coalition was instrumental in working alongside consumer groups to educate the offices of Senators Herb Kohl (D-WI), Amy Klobuchar (D-MN), and Richard Burr (R-NC) regarding accounting of disclosures. Subsequently, HLC was referenced in the letter from senators Kohl and Klobuchar to HHS Secretary Kathleen Sebelius.
- The Confidentiality Coalition has met with administration officials from the White House, the Office for Civil Rights (OCR), and HHS regarding the accounting of disclosures NPRM.
- The Confidentiality Coalition met with members of the Senate Commerce Committee and House Energy and Commerce Committee regarding the need for a HIPAA carve-out in pending data security legislation.
- In June, the Confidentiality Coalition hosted IMS Health to discuss the results of a 2011 survey on voters' attitudes and concerns on privacy and health information and to engage Steering Committee members in a discussion regarding messaging efforts.
- The Healthcare Leadership Council (HLC) joined former HHS Secretaries Tommy Thompson and Dr. Louis W. Sullivan in filing an amicus brief with the U.S. Supreme Court in *Sorrell v. IMS Health Inc.* It urged the justices to strike down state laws that raise unnecessary barriers obstructing the flow of important healthcare information. In June, the Supreme Court struck down the Vermont law.
- In April, members of the Confidentiality Coalition met with the staff of Senator John Kerry (D-MA) to discuss how healthcare research would be affected under his "Commercial Privacy Bill of Rights" (S. 799).
- In March, Confidentiality Coalition members met with staff from Representative Jackie Speier's (D-CA) office to discuss her online privacy bill, the "Do Not Track Me Online Act of 2011" (H.R. 654).
- The Confidentiality Coalition also met with staff from Representative Mary Bono Mack's (R-CA) office to discuss her interest in consumer privacy, given her new role chairing the House Subcommittee on Commerce, Manufacturing, and Trade.
- The Confidentiality Coalition filed a public comment letter with the FTC in connection with its preliminary staff report entitled "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The letter emphasized that a dual oversight regime on health privacy should not be imposed upon HIPAA-regulated organizations.
- House majority staff on committees of jurisdiction over HIPAA has asked the Confidentiality Coalition to provide regular feedback on privacy issues related to the administration's implementation of the HITECH Act.
- The Confidentiality Coalition has been represented at HHS HIT Policy Committee meetings during the public comment period to express concern about the potential overreach of privacy recommendations coming from the committee.

- The Confidentiality Coalition continues to work with individual members of the HHS “tiger team” on privacy and security to educate them on concerns related to informed consent for treatment, payment, and healthcare operations, and to explain the necessity of information flow to improve healthcare quality and outcomes.