CONFIDENTIALITY COALITION

Advancing Health Care. Safeguarding Trust.

Legislative and Regulatory Issues and Coalition Activity

2010

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 2009 federal stimulus law amended HIPAA by creating additional health privacy provisions for these and other organizations that handle health information. Though the HIPAA Privacy Rule established federal policy, it permits significant state variation that makes complying with all applicable rules unnecessarily complex and presents a barrier to the necessary transmittal of health information.*

Position: *The Confidentiality Coalition believes the confidentiality of health information is vital to engendering trust in the healthcare system; however, it is critical that the federal government guards against enacting legislation or establishing regulations that would hamper efforts to provide safe, high-quality, and coordinated healthcare. 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 HHS Privacy Rule the uniform national standard, replacing the conflicting patchwork of state privacy laws.*

Regulatory and Legislative Action in 2010:

- In 2010, the Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) continued to promulgate rules to implement the HIT provisions (HITECH) 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.
- At the end of 2009, the Office of the National Coordinator for Health Information Technology (ONC) announced a reorganization of its operational structure to better support the implementation of the health information technology (HIT) goals articulated in ARRA. The reorganization created five new offices, including the Office of the Chief Privacy Officer.

- In August of 2009, HHS published the interim final rule for breach notification by covered entities and business associates.
    - On February 22, 2010, the HHS Office for Civil Rights (OCR) began enforcing the Breach Notification Interim Final Rule. OCR had previously announced that it would not use its enforcement discretion to impose fiscal sanctions for breaches of PHI discovered before February 22, 2010.
    - On July 28, OCR announced that it was withdrawing the breach notification final rule from the Office of Management and Budget (OMB).
- The notice of proposed rulemaking on "meaningful use" of HIT was published in the Federal Register on January 13, 2010. ONC published a closely related interim final rule in early January that specifies the adoption of an initial set of standards, implementation specifications, and certification criteria for EHRs. National Coordinator for Health Information Technology Dr. David Blumenthal stated that issues of privacy and confidentiality are foundational to all of the work ONC is doing.
- In February 2010, Joy Pritts, a lawyer, privacy researcher, and Georgetown University faculty member, was named the first chief privacy officer to ONC. Pritts will advise ONC on data privacy and security issues.
- In early March, OCR held a two-day workshop on the HIPAA Privacy Rule's de-identification standard. The purpose of the workshop was to solicit stakeholder input to inform OCR's development of guidance on methods for de-identification of "protected health information" (PHI), as newly required by ARRA. The workshop consisted of several panels, each of which addressed a specific topic related to the Privacy Rule's de-identification methodologies and policies.
- The FTC has recently expanded its involvement in consumer privacy issues with a series of public roundtable discussions to explore the privacy challenges posed by technology and business practices that collect and use consumer data. The third and final roundtable was held on March 17.
- On March 24, ONC released a paper as part of its Privacy and Security Whitepaper Series titled, "Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis." It examines in detail the issues and tradeoffs of various consent options for electronic health information exchange.
- On May 3, OCR issued a Request for Information (RFI) asking for additional information on a variety of issues regarding accounting of disclosures (AOD), including the usefulness of an AOD report, as well as technological capabilities to produce an AOD report.
- On May 4, Representatives Rick Boucher (D-VA) and Cliff Stearns (R-FL) released a discussion draft of proposed internet privacy legislation. The bill stipulates notice and consent requirements for the collection, use, and disclosure of personally identifiable information transmitted via the internet.
- In June, ONC announced the organization of a subcommittee under the auspices of the HIT Policy Committee to move forward quickly on a range of privacy and security issues. ONC expects the work of the Privacy and Security "Tiger Team" to be completed by late fall.
- On June 29, the Privacy and Security Tiger Team held a hearing on consumer choice technologies to discuss technologies that enable consumers to choose whether or not to share their information in health information exchange.
- The final rule on "meaningful use" of HIT was published in the Federal Register on July 13, 2010. ONC published a closely related final rule the same day that specifies

the adoption of an initial set of standards, implementation specifications, and certification criteria for EHRs. National Coordinator for Health Information Technology Dr. David Blumenthal has stated repeatedly that issues of privacy and confidentiality are foundational to ONC's efforts to create a nationwide interoperable electronic health information system.

- On July 14, HHS published a notice of proposed rulemaking (NPRM) encompassing many of the remaining health privacy-related issues from HITECH. As a result of the "omnibus" NPRM, privacy and security rules governing health information will include broader individual rights and stronger protections when third parties handle individually identifiable information.
- A number of consumer protection and Internet privacy bills were introduced in 2010 in both the House and Senate. On July 27 the Senate Commerce Committee held a hearing titled "Consumer Online Privacy" that examined how consumer information is gathered and shared online.
- In August, the Tiger Team recommended to the HIT Policy Committee that patients be able to exercise "meaningful consent" regarding participation in electronic information exchange when certain conditions are present.
- On September 22, the Senate Committee on Commerce, Science, and Transportation held a legislative hearing on S. 3742, the "Data Security and Breach Notification Act of 2010."
- In October, an HHS Office for Civil Rights (OCR) official said the agency hopes to release a final rule to implement changes to the HIPAA privacy, security, and enforcement rules in late 2010 or in early 2011. OCR is reviewing over 500 comments the department received on the proposed rule, which was published in July.
- As of October 5, OCR reports that, for breaches affecting over 500 individuals, 176 breach reports have been posted on its website. For breaches involving fewer than 500 individuals, OCR has received over 9,250 breach reports that affect more than 40,000 people.
    - In conjunction with the omnibus privacy NPRM, HHS redesigned its breach website. As required by the HITECH Act, HHS publishes a list of breaches of unsecured PHI affecting 500 or more individuals on the OCR website. The updated website allows the public to identify more easily where and what kinds of breaches have occurred, and includes summaries of breach cases that have been investigated and closed by the department.
- On October 5, the Office of Personnel Management (OPM) published a notice in the Federal Register announcing its intent to launch a central and comprehensive database designed to track federal employee health benefit plans, and monitor and evaluate the cost and quality of services provided. Consumer privacy groups have expressed concern about the use and protection of such data.
    - On November 15, OPM announced it would delay the launch of the Federal Health Claims database until December 15 to accommodate public comments.
- On October 20, the ONC Privacy and Security Tiger Team presented recommendations regarding transparency to the HHS HIT Policy Committee. The Tiger Team's recommendations included a new core value for the Policy Committee's consideration stipulating that "transparency about information exchange practices is a necessary component of establishing credibility with patients."

- On October 24, the White House National Science and Technology Council announced the launch of a new Subcommittee on Privacy and Internet Policy. The subcommittee will develop principles and strategic directions with the goal of fostering consensus in legislative, regulatory, and international Internet policy realms, which could include online health data. The subcommittee will include a representative from HHS, as well as officials from other federal agencies.
- On November 9, the Equal Employment Opportunity Commission published final regulations implementing Title II of the Genetic Information Nondiscrimination Act (GINA), which bans employment discrimination based on an individual's genetic information and family medical history. The final regulations will take effect January 10, 2011.
- Per the HITECH Act, the Substance Abuse and Mental Health Services Administration (SAMHSA) is conducting a Confidentiality and Privacy Issues Related to Psychological Testing Data study, in close cooperation with OCR. As part of this study, SAMHSA hosted public meetings to bring together professionals in the areas of mental health and privacy protection to discuss current practices and the policy implications. The first meeting was held October 7 in Chicago, Illinois, and the second November 18 in Los Angeles, California.
- On December 1, the Federal Trade Commission (FTC) released a draft privacy report calling for greater online consumer protections that touch on the health information technology (HIT) industry. The report proposes a framework for how companies should protect consumers' privacy. Comments will be accepted on the components of the proposed framework until January 31. The FTC plans to release a final report in 2011.
    - On December 2, the Subcommittee on Commerce, Trade, and Consumer Protection of the House Energy and Commerce held a hearing entitled "Do-Not-Track Legislation: Is Now the Right Time?" The hearing examined the feasibility of establishing a mechanism that provides Internet users a simple and universal method to opt-out from having their online activity tracked by data-gathering firms.
- On December 3, the HHS Office of National Coordinator for Health Information Technology (ONC) hosted a public roundtable on "Personal Health Records — Understanding the Evolving Landscape." Panelists highlighted the need for providers and payers to give individuals more access to and control over their personal medical information.
    - On November 3, ONC posted a request for public comment to gauge privacy and security concerns surrounding personal health records (PHRs) in preparation for its December 3 PHR roundtable.
- On December 8, the President's Council of Advisors on Science and Technology released a report titled "Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward." The report calls for the development of "universal exchange language" to facilitate health data sharing while strengthening the privacy and security of health information.
- On December 9, the HHS HIT Policy Committee's privacy and security "tiger team" held a public hearing on patient matching, which involves ensuring that the patient is properly identified and correctly linked to the rest of his or her data in health information exchange between healthcare organizations. The tiger team gave an overview of the hearing to the HHS HIT Policy Committee at its December 2010

meeting, and is formulating formal recommendations to present to the entire HIT Policy Committee at a future meeting.

- The HITECH Act requires covered entities that use or maintain an electronic health record (EHR) to provide, upon request, an accounting of disclosures made for treatment, payment, and healthcare operations purposes through an EHR over a three-year period. This provision expands significantly a HIPAA Privacy Rule requirement that physicians, hospitals, and other covered entities prepare an accounting of all "non-routine" disclosures of a patient's personal health information. Accounting of disclosures was not included in the omnibus privacy NPRM, but a separate rule is expected to be published on this matter later this year.
- In addition, guidance is forthcoming on implementing requirements for the de-identification of protected health information, as well as a final rule for breach notification for unsecured health information.

Background and Additional Detail:

Passage in early 2009 of the economic recovery package, ARRA, included $22 billion in long-awaited HIT funding. It also included expansion of health privacy requirements. HHS has released several interim final rules and notices of proposed rulemaking implementing many of the new privacy and security provisions, such as breach reporting and strengthening the civil and criminal enforcement of the HIPAA Privacy and Security Rules. The "omnibus" privacy NPRM released in July largely incorporated the HITECH statutory changes into the Privacy and Security Rules of HIPAA.

As expected, the proposed rule extends privacy and security requirements governing the treatment of protected health information (PHI) to business associates of healthcare entities. New categories have been added to the definition of a business associate, such as health information exchanges, as identified in the HITECH law. Notably, however, the proposed rule also extends the HIPAA Privacy and Security Rule requirements to subcontractors of business associates. Furthermore, both business associates and their subcontractors will be subject to HIPAA liability. The new HITECH obligations for business associates will become applicable 180 days after the effective date of the final rule, which is expected in early 2011.

The NPRM also addressed a number of remaining ARRA privacy and security regulatory issues. HHS proposes to:

- Require authorization for any marketing communications that generate "direct or indirect payment" for the covered entity, a change from the original HIPAA marketing rule. However, the rule fails to define "direct or indirect payment." Authorizations are not required for treatment-related marketing communications, but patients must be given the opportunity to opt out of receiving such communications.
- Incorporate the HITECH provision requiring an authorization for any sale of PHI involving "direct or indirect remuneration." It did not discuss the definition of "direct or indirect."
- Require covered entities to restrict disclosure of PHI that relates to a specific treatment to a health plan where the patient has paid for services out-of-pocket. The NPRM included little discussion regarding this provision.

- Provide individuals a right to obtain a copy of their personal health information contained in an electronic record in an electronic format. If the information exists only in a paper format, the covered entity is not required to create an electronic record.

HITECH provisions that were not included in the privacy omnibus NPRM include a final rule for breach reporting and guidance on the HIPAA-mandated "minimum necessary" standard for exchange of PHI.

Separate regulation requiring covered entities to account for disclosures of protected health information via an electronic health record for treatment, payment, and healthcare operations for a period of three years is also forthcoming. In addition to the Request for Information published May 3 in the Federal Register, OCR hosted a series of meetings in May with consumer groups to assess consumer interest in and the benefits of AOD reports, as well as with technology experts to discuss current software capabilities. OCR previously met with provider groups in November 2009 to assess the impact of the expanded regulations on healthcare providers.

CMS published its notice of proposed rulemaking on "meaningful use" of HIT in the Federal Register on January 13, 2010. ONC published a closely related interim final rule in early January that specifies the adoption of an initial set of standards, implementation specifications, and certification criteria for EHRs. Providers must use certified EHRs in order to be eligible for Medicare incentive payments. Certified EHRs are required to protect electronic health information by implementing encryption and other controls; however, HHS underscored the fact that certification alone does not equate to compliance with the HIPAA Privacy or Security Rules.

The HHS HIT Policy and Standards Committees, whose work informed the development of the regulations published by CMS and ONC, continue to meet to develop recommendations for meaningful use objectives and measures for subsequent stages of the incentive program. The incentive program is a three-stage effort, with measures and objectives becoming more robust as the program progresses.

At the May 19 HIT Policy Committee meeting, the Privacy and Security workgroup recommended data encryption for one-to-one exchanges of patient information for treatment purposes. The workgroup recommended the encryption policy in lieu of requiring patient consent for the direct exchange of personal health information between providers. Such a recommendation would have to be implemented either through meaningful use regulation or related certification criteria, or through a change to the HIPAA Security Rule.

In June, ONC announced the organization of a subcommittee under the auspices of the HIT Policy Committee to move forward on a range of privacy and security issues, particularly guidance for State Health Information Organizations, on topics affecting information exchange. This Privacy and Security "Tiger Team" is comprised of members from the HIT Policy and Standards Committees, as well as the National Committee for Vital Health Statistics (NCVHS). The Tiger Team has met regularly and intensely since June to consider how best to build public trust and participation in health information technology (HIT) and

electronic health information exchange by incorporating effective privacy and security into every phase of HIT, adoption, and use.

In August, the Tiger Team submitted additional recommendations to National Coordinator David Blumenthal, chairman of the HIT Policy Committee, regarding the electronic exchange of patient-identifiable health information among entities to meet Stage 1 of meaningful use. Building upon a previous recommendation to the HIT Policy Committee that direct provider-to-provider exchange for treatment should not require patient consent, the Tiger Team also recommended that patients be able to exercise "meaningful consent" regarding participation in electronic information in certain identified circumstances.

On October 20, the Privacy and Security Tiger Team presented recommendations regarding transparency to the HIT Policy Committee. The Tiger Team struggled with how to effectively inform patients about how their personal health information is shared in a manner that is manageable for patients, without unduly burdening providers. The Tiger Team recommended a layered, "tiered" approach to transparency that includes both a short summary of sharing policies and activities, as well as more detailed notice to be provided to patients upon request. The Tiger Team recommended that communication regarding transparency be applied to three contexts: 1) the HIPAA Notice of Privacy Practices; 2) any exchange that triggers meaningful consent, per its August recommendations; and 3) Organized Health Care Arrangements and other integrated delivery networks. The transparency recommendations were not approved by the full HIT Policy Committee in October; ultimately, they will serve as an initial set of recommendations which the HIT Policy Committee will build upon as it continues to work on transparency. The Tiger Team is expected to address issues regarding provider authentication and digital credentials in the coming months.

Numerous bills in both the House and Senate were introduced in 2010 to provide consumer protections in the online collection and storage of personal information and to mandate security procedures to prevent breaches of this information. On August 5, Senators Mark Pryor (D-AR) and John Rockefeller (D-WV) released the ''Data Security and Breach Notification Act of 2010'' (S. 3742), which requires security policies and procedures to protect data containing personal information. Senator Patrick Leahy (D-VT) also has a long-standing data security bill (S. 1490, the "Personal Data Privacy and Security Act of 2009") that has been passed out of the Judiciary Committee. Both Senate bills address the security of health information and have breach provisions included. Each bill needs a comprehensive HIPAA exemption for both covered entities and business associates; otherwise, the FTC and HHS can dually regulate these healthcare organizations. The Obama administration earlier this fall put pressure on committee chairmen Leahy and Rockefeller to merge their bills and introduce one, comprehensive data security bill, which could go to the Senate floor during the "lame duck" session in December.

On the House side, on July 22, Representative Bobby Rush (D-IL) introduced the "BEST PRACTICES Act" (H.R. 5777), designed to heighten protections of consumers' personal information. This bill has been referred to the Committee on Energy and Commerce. There is similar concern that this bill lacks adequate exemption language for HIPAA-covered entities. If there is movement toward final passage of this bill and a merged Senate bill, these two bills would be conferenced to produce final data security legislation.

The FTC has recently expanded its involvement in consumer privacy issues. Its "Exploring Privacy" roundtable series was developed to determine how best to protect consumer privacy while supporting beneficial uses of the information and technological innovation. Roundtable panels featured experts in their fields and focused on risks and benefits of information-sharing practices, consumer expectations regarding such practices, behavioral advertising, information brokers, and the adequacy of existing legal and self-regulatory frameworks. The March 17 roundtable included a panel specific to health information, and personal health records, in particular. Questions were made available for public comment prior to each of the roundtables. The FTC reviewed the public comments received in conjunction with the privacy roundtables series and issued its preliminary report in early December.

The preliminary report released December 1, "Protecting Consumer Privacy in an Era of Rapid Change," is based upon the major themes and concepts elucidated through the roundtables. The report proposed a framework for businesses and policymakers to better protect consumers' privacy and contained three main components: 1) privacy by design: companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services; 2) simplified choice: companies should simplify consumer choice and allow for more meaningful choice with respect to data practices that are not commonly accepted practices; and 3) greater transparency: companies should increase the transparency of their data practices. Comments will be accepted on the components of the proposed framework until January 31, 2011, and the FTC will publish a final report later this year.

Confidentiality Coalition Activity in 2010:

- HLC, through the Confidentiality Coalition, works closely with key legislators and regulators to ensure HIPAA-related privacy legislation does not impede efforts to provide safe, high-quality, and coordinated healthcare.
- HLC continued to grow and diversify the Confidentiality Coalition in 2010 and has been successful in garnering support from national patient groups.
- Incoming majority staff on committees of jurisdiction over HIPAA have asked the Confidentially Coalition to provide regular feedback on privacy issues related to the administration's implementation of the HITECH Act.
- The Confidentiality Coalition has been asked by Republican staff on the House Ways and Means Committee to conduct a HIPAA privacy briefing to educate new members and staff in the 112th Congress.
- HLC coauthored an article in the November issue of *Health Affairs* on comparative effectiveness research and privacy policy.
- On November 4, Confidentiality Coalition members met with key staff of the House Ways and Means Committee to discuss concerns that the Tiger Team is de facto rewriting HIPAA under the guise of meaningful use policy.
- In November, the Confidentiality Coalition submitted a letter of support for a nominee to the National Committee on Vital and Health Statistics (NCVHS).
- In October, members of the Confidentiality Coalition met with staff of Senators Mark Pryor (D-AR) and Roger Wicker (R-MS) (Senate Commerce Committee sub-chairmen) to offer suggested HIPAA carve-out language for the "Data Security and Breach Notification Act of 2010" (S. 3742).
- In October, the Confidentiality Coalition provided comments in response to the Tiger

Team's request for information on provider authentication and digital credentials, as related to the exchange of electronic health information.

- In October, the Confidentiality Coalition hosted a briefing on the impact of the HITECH Act on marketing and research conducted by pharmaceutical companies.
- In September, the Confidentiality Coalition compiled a list of real-world examples that illustrate the effectiveness of the risk-based standard for breach notification, as well as steps that covered entities have taken to comply, to share with OCR staff and other HHS officials.
- HLC staff regularly work with HLC member organizations to educate them on issues related to privacy and security policy.
- 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.
    - For example, the Confidentiality Coalition hosted Deven McGraw, director of the Health Privacy Project at the Center for Democracy and Technology (CDT) and co-chair of the HHS Privacy and Security Tiger Team, to discuss the ongoing discussions and recommendations of the Tiger Team.
- In September, the Confidentiality Coalition submitted comments on the omnibus privacy NPRM.
- Mary Grealy and HLC staff met with ONC Chief Privacy Officer Joy Pritts in late August to discuss evolving privacy policy developed by HHS.
- HLC serves as a resource to prominent media outlets for stories related to federal privacy policies.
- In July, HLC held a privacy briefing to review the NPRM on modifications to the HIPAA Privacy, Security and Enforcement Rules.
- The Confidentiality Coalition responded to Representative Rick Boucher's request for revisions to his proposed Internet privacy legislation, focusing on a clear HIPAA exemption for healthcare organizations.
- On May 18, the Confidentiality Coalition filed a response to OCR's request for information on the expanded accounting of disclosures requirements. The comment letter highlighted the dearth of requests for AOD reports, the lack of utility to the average patient, and current technological limitations.
- On May 6, the Confidentiality Coalition participated in the technology stakeholder meeting with OCR to discuss the lack of current technical solutions to automatically generate AOD reports and to distinguish between "uses" and "disclosures" of health information.
- The Confidentiality Coalition is developing a strategic action plan regarding informed consent, particularly in regard to consent for purposes of treatment, payment, and healthcare operations.
- In March, the *Wall Street Journal* printed Mary Grealy's letter to the editor regarding healthcare privacy regulation as it relates to the essential flow of medical information to improve healthcare quality and increase safety.
- The Confidentiality Coalition developed a set of principles for de-identification that were shared with OCR at its March stakeholder meeting.
- The Confidentiality Coalition filed a public comment letter to the FTC emphasizing that a dual oversight regime on health privacy should not be imposed upon HIPAA-regulated organizations.
- The Confidentiality Coalition hosted FTC staff at the March coalition meeting to

discuss FTC's recent involvement in privacy and data security enforcement efforts.

- HLC worked with Hill offices to craft health reform language that identifies regulatory barriers affecting the necessary flow of medical information.
- Through its chairing of the Confidentiality Coalition, HLC advocated for balanced and thoughtful updates to federal privacy policy during the ARRA debate and served as a key resource to Senate and House offices on issues related to privacy.
-