HIPAA and Beyond: The Evolving Landscape of Health Privacy

Melissa Bianchi, Hogan Lovells US LLP
Ann Tobin, UnitedHealth Group

IAPP Global Privacy Summit, March 9, 2012
No Longer Just HIPAA

- New developments that are changing the regulatory landscape for healthcare companies regulated by HIPAA
  - Changes to and expansion of HIPAA
  - Activities by other agencies that could broaden regulation of healthcare companies
  - New technologies (e.g., mobile health, website use) that raise novel regulatory issues for healthcare companies
Expansion of HIPAA

- Expecting Final HIPAA rules – first quarter of 2012?
- Beyond the Office for Civil Rights – HHS is expanding privacy and security requirements for HIPAA covered information.
  - Office of Human Subjects Research Protections
    - An Advanced Notice of Proposed Rulemaking (ANPRM) issued in 2011 regarding human subjects research and secondary uses
  - Office of the National Coordinator
    - Meaningful Use
    - Health Information Exchange
  - Reconsideration of de-identification standards within HIPAA and beyond
  - State Attorneys General
Rules on Human Subjects Research

- ANPRM published in July 2011
- Contained proposed requirements for human subject research that, if adopted, would:
  - Require research entities to apply HIPAA-like privacy and data security standards to all studies involving identifiable or potentially identifiable data
  - Restrict the ability to use information for future research purposes; change rules for biospecimens
EHRs – Meaningful Use

- Proposed rules for Stage 2 of the Meaningful Use program will be released early this year
- Office of the National Coordinator for Health IT (ONC) is already working on Stage 3
- Future stages of meaningful use may impose privacy and security requirements on EHRs
  - Already additional security requirements for certified EHRs
  - More changes possible as these programs move from merely storing health information toward HIEs
Health Information Exchange

- States have received funding and are creating their own HIEs
- Focus of ONC in 2012
- ONC is preparing ANPRM on governance of the Nationwide Health Information Network (NWHIN)
  - May include privacy and security guidance for health information exchange, including:
    - Security requirements
    - Rules on consent
New Concepts of De-identification

- HHS work on de-identification
  - HHS de-identification guidance
  - ANPRM on human subjects research

- Consistent with changing approach to de-identification outside of HHS
  - Expansive EU concept of personal data
  - Preliminary FTC report foreshadows broader definition in US
Other Federal Activities

Beyond HHS, other federal agency and legislative activities affect entities subject to HIPAA

- FTC activities
- Privacy legislation
The final FTC report is expected to outline what the FTC expects companies to do as “best practices” when it comes to privacy.
- HIPAA covered entities will have HIPAA notice of privacy practices and website privacy policy

FTC Enforcement:
- In 2009/2010 FTC brought two high-profile enforcement actions against CVS and RiteAid
- Violation of Section 5 of FTC Act for improper storage/disposal of PHI
- Settlements require establishment of comprehensive security programs
- Settlements require third-party security assessment every other year
Federal Legislation

Congress considered dozens of bills in 2011, including:
- Comprehensive privacy legislation
- Federal data breach

Effect on entities already subject to HIPAA:
- Safe harbor for HIPAA covered entities? Business associates? Information covered by HIPAA?
Mobile Privacy

- New landscape for HIPAA covered entities (disease management)
- Areas beyond HIPAA covered entities: employee data, pharmaceutical companies, federal government guidance re: texting, etc.
Mobile Privacy, cont.

- WSJ 12/10 article on mobile app privacy, reporting that of 101 popular smartphone apps, 45 didn’t even have a privacy policy and others transmitted information without consumer consent
- Almost immediately thereafter, multiple class action lawsuits were filed against Apple, Google, and mobile app developers and advertisers
  - These lawsuits have foundered due to a failure of plaintiffs to prove financial harm
  - Still, have been costly and highlights the focus on mobile privacy
- 2011 saw FTC bring first enforcement actions against mobile app developers
- FTC to hold mobile payments workshop in April, focusing on risks to privacy and security of mobile data
BOTTOM LINE: From a privacy and security perspective, mobile devices should be treated the same as computers, and mobile apps should be treated the same as websites

- Additional considerations: sensitivity of location data, unique device identifier, other information stored locally on smartphones (e.g., address book, contacts)
Website Data Practices

- Moving data to the cloud – trusting vendors with your privacy and security compliance
- Continued focus on web tracking and third-party marketing
- Enforcement efforts look at language in privacy policies
Electronic Signatures

- **Federal standard (ESIGN)**
  - In 2000 Congress enacted the Electronic Signatures in Global and National Commerce Act (“ESIGN”)
  - Aimed at facilitating the use of electronic records and electronic signatures in interstate and foreign commerce
ESIGN expressly allows states to “modify, limit, or supersede” the federal statute if states adopt the Uniform Electronic Transactions Act (UETA) or adopt an electronic transactions law that is consistent with ESIGN.

The UETA provides that “[a] record or signature may not be denied legal effect or enforceability solely because it is in electronic form” - UETA § 7(a).

47 states, the District of Columbia, Puerto Rico, and the Virgin Islands have adopted the UETA.

Illinois, New York, and Washington have not adopted the UETA, but do have laws pertaining to electronic transactions.
General Requirements for Electronic Signatures

- **Assent and Consent** – Both parties must agree to the use of electronic signatures
- **Authentication** – There must be a mechanism to authenticate the parties to an electronic transaction
- **Record Retention** – Consumers must be provided a reasonable means to retain the relevant electronic agreement or notice
In Conclusion

- Watch for changes to and expansion of HIPAA by HHS, including OCR, OHRP, ONC
- Watch for continuing activity of other agencies affecting healthcare companies—e.g., FTC
- Landscape will continue to change and develop with mobile health and other new technologies
• ANPRM for Revisions to Common Rule
• FTC—CVS/Caremark Matter
• HHS—CVS/Caremark Matter
• FTC—Rite Aid Matter
• HHS—Rite Aid Matter
• Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (December 1, 2010)
• HHS mHealth Initiatives
• MN Attorney General Complaint against Accretive Health
• HHS Office of National Coordinator HIT
Questions & Contact Information

Melissa Bianchi  
Partner  
Hogan Lovells US LLP  
melissa.bianchi@hoganlovells.com  
202-637-3653

Ann Tobin  
Senior Privacy Counsel  
UnitedHealth Group  
an_e_tobin@uhc.com  
952-936-7236