Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

January 2013 - Issue 24

What's Inside?

Big Data, Healthcare and Privacy

Social networking sites, e-commerce and electronic medical records continue to fuel exponential growth in electronic data. Big data—large volumes of electronic data that can be captured, communicated, aggregated, stored, and analyzed—is now part of every sector of the global economy. Healthcare is an important segment of the U.S. economy that faces tremendous productivity challenges. Stakeholders include providers, payers, patients and researchers as well as drug and medical device companies. These stakeholders, with different interests/business incentives, generate data sets which usually remain separate and distinct. There is potential to create value if these data silos can be digitized and combined. This data includes patients' records held by multiple doctors/hospitals, information only patients know (e.g., behaviors, life and job histories), newly available genetic information and health data generated by researchers, drug companies and insurers. This protected health information (PHI) as defined by the HIPAA regulations, is highly sensitive and thus requires protection from inappropriate access/disclosure. Yet, the ability for researchers to combine and analyze these huge data sets significantly increases the probability of discovering causes and developing effective treatments for all types of health conditions.

Frequently Asked Question

Q: How long should University records be retained?

A: Retention periods for University records vary depending on category and type. Consult the University Document Retention Policy and Retention Schedule for specific retention periods. Additional questions can be addressed to General Counsel and Records Management.

Have a Question?

hipaaprivacy@med.miami.edu

Prior newsletters available online
http://www.privacyoffice.med.miami.edu

However, having all their health data electronically stored and potentially accessible by multiple, "unknown" entities alarms many patients and privacy advocates. Privacy protections are about building a healthcare ecosystem that people will trust. When patients seek care, especially regarding sensitive issues, they must be reasonably assured that information will not be shared outside of those who have a need to know, e.g. insurance companies/providers. They must also have confidence in security mechanisms in place to prevent "hackers" or other unauthorized individuals from accessing such information. This is essential to respect patient privacy and build patient trust. If we are unable to provide some reasonable assurance about how their data is used, many individuals could decline to seek care, patronize other providers who can demonstrably provide such assurances or not fully reveal health conditions when truthfulness is important. Finally, privacy issues will surface as data analytics provides the ability to reveal individual identities by combining what was previously considered "anonymous data" with "new" data pools such as location and purchasing information.

Health Insurance Exchanges Create New HIPAA Challenges

Hospitals/health plans that intend to participate in state insurance exchanges under the Affordable Care Act are likely to find a host of new privacy/security requirements. Since the act has been upheld, most states are moving forward as the law requires exchanges be established by January 2014. Some states will operate their own exchanges while others will establish exchanges through partnerships with the government and its contractors. Exchanges will facilitate the purchase of health insurance coverage by small business and individuals, with functions from determining eligibility and vetting plans for compliance with required benefits to making plans available online and processing enrollments. In most cases, the exchanges themselves will not be covered entities (CEs) under HIPAA, falling instead under the federal Privacy Act and relevant state laws, among others. HHS regulations issued in March 2012 made it clear that the agency did not mandate exchanges to be CEs, but this would depend on governance issues and the information being exchanged. Participating insurers/qualified health plans will continue to be CEs, and must continue to comply with HIPAA, as well as new privacy and security measures that exchanges choose to implement. The final rule adopted the proposed rules' provisions for protecting patient information, which require exchanges to adopt "safeguards that ensure a set of critical security outcomes" and lay out the "framework within which an exchange must create its privacy and security policies and protocols." The rule states a "need for flexibility in the implementation of these standards in order to minimize implementation costs." HHS chose not to "establish a single, baseline standard" but is directing exchanges to develop privacy and security policies based on FTC Fair Information Practice Principles. One aspect that all exchanges must address is giving patients some control over their information.

Office of HIPAA Privacy & Security
Professional Arts Center (PAC), Suite 409 (M-879)
http://www.privacyoffice.med.miami.edu
Phone: 305-243-5000
Fax: 305-243-7487

PRIVACY & SECURITY NEWS

Massachusetts Provider Settles HIPAA Case for $1.5 Million

Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. (MEEI) has agreed to pay the U.S. Department of Health and Human Services' (HHS) $1.5 million to settle potential violations of the HIPAA Security Rule. MEEI also agreed to take corrective action to improve policies and procedures to safeguard the privacy and security of its protected health information (PHI). The investigation by the HHS Office for Civil Rights (OCR) followed the theft of an unencrypted laptop containing the health information of MEEI patients and research subjects. The information lost included patient prescriptions and clinical information. OCR's investigation indicated that MEEI failed to conduct a thorough risk analysis of ePHI maintained on portable devices and implementing policies and procedures to address security incident identification, reporting, and response. In addition to the $1.5 million settlement, the agreement requires MEEI to adhere to a corrective action plan which includes reviewing, revising and maintaining policies and procedures to ensure compliance with the Security Rule, and retaining an independent monitor who will conduct assessments of MEEI's compliance with the corrective action plan and render semi-annual reports to HHS for a three year period.

Massive Data Breach Costs South Carolina $20 Million +

Social Security Numbers (SSN) belonging to about 3.6 million residents in South Carolina have been exposed in a computer intrusion at the state's Department of Revenue. Another 387,000 credit and debit card numbers were also exposed in the September 2012 attack. Anyone who has filed a South Carolina tax since 1998 has been impacted by the breach and will be offered identity protection services from Experian. The service includes a $1 million identity theft insurance policy. More than three months later the state is still working on securing computer systems and notifying victims. Currently the price tag for the breach is $20 million and counting. The amount which includes credit monitoring, security upgrades and consultants – is expected to increase when other state agencies submit requests to bolster their computer systems. Gov. Nikki Haley's executive budget included at least another $16.6 million in breach-related requests. "The number of records breached requires an unprecedented, large-scale response by the Department of Revenue, the State of South Carolina and all our citizens," South Carolina Gov. Haley said. "We are taking immediate steps to protect the taxpayers of South Carolina, including providing credit monitoring and identity protection to those affected."

Shareholder Proposal Asks Apple for Privacy Risk Report

A group of Apple's investors have filed a shareholder proposal seeking a report on how the company's board of directors governs privacy and data security vulnerabilities, according to an OpenMIC press release. The proposal states that "Apple's board has a fiduciary and social responsibility to protect company assets, which include the personal information of a variety of stakeholders." The two groups co-filing the proposal cite a number of recent cybersecurity and privacy incidents affecting the company and refer to a Carnegie Mellon University CyLab study by Jody Westby that looked into how executives manage cyber risks. "My Cylab governance surveys indicate the governance by boards and senior management is not where it should be," Westby told the Daily Dashboard, adding, "This type of shareholder inquiry cannot be ignored or passed down the line by senior management."

Lack of Email Privacy Protection

In an op-ed for Time magazine, Adam Cohen discusses the lack of legal ground in the U.S. for email privacy protection. He writes that many in government "like the idea of being able to read citizens' private email" and Internet users have "gotten good at pushing back against Facebook over privacy issues" while not putting pressure on lawmakers to "strengthen email privacy." The scandal that brought down General David Petraeus last fall contained a mini-scandal within it: just how easy it is for the FBI to read people's email. Meanwhile, Financial Times opines, "The technology underlying the surveillance economy is evolving faster than the ability of social norms to adapt, or regulators to keep pace." Four basic rights are called for: notice, anonymity, redress and data portability.

Related Links

- **Massachusetts Provider Settles HIPAA Case for 1.5 Million:** http://www.hhs.gov/news/press/2012pres/09/20120917a.html
- **Massive Data Breach Costs South Carolina $20 Million +:** http://www.charlotteobserver.com/2013/01/06/3769853/sc-continues-notifying-data-breach.html
- **Shareholder Proposal Asks Apple For Privacy Risk Report:** http://www.natlawreview.com/article/apple-shareholders-request-information-board-privacysecurity-risk
- **Lack of Email Privacy Protection:** http://ideas.time.com/2013/01/02/the-government-would-like-to-keep-reading-your-email/

Office of HIPAA Privacy & Security
Professional Arts Center (PAC), Suite 409 (M-879)
http://www.privacyoffice.med.miami.edu
Phone: 305-243-5000
Fax: 305-243-7487