Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

August 2012 - Issue 23

What's Inside?

Meaningful Use - Privacy & Security Are Not Optional

The HITECH Act authorizes incentive payments through Medicare/Medicaid to hospitals/providers who meet "Meaningful Use" (MU) criteria by using certified electronic health records (EHRs) to achieve healthcare improvements. MU requirements will be phased in through three stages over the next several years. Stage 1 focuses on the use of a certified EHR. Stages 2 and 3 encourage use and exchange of electronic health information. For any questions about UHealth's MU initiative, please contact Mike Kelley, Vice Chair for Administration, University of Miami Medical Group, at 305-243-3062 or mkelly@med.miami.edu.

So where does privacy and security fit into these requirements? Patients who trust that their health information will be kept private and secure, are much more likely to discuss their symptoms, conditions, as well as past and present risk behaviors. Therefore, protecting patients' privacy and securing their health information is a core requirement for "Meaningful Use". Trust is clinically important and a key business asset. Secure handling of patient information and sensitivity to privacy concerns can be an important tool in a competitive healthcare environment.

Stage 1 requires a security risk analysis to comply with the HIPAA Security Rule, and implementing updates as necessary. CMS has also issued the Stage 2 MU notice of proposed rule-making with additional privacy/security requirements. The proposed rule explicitly includes "addressing the encryption/security of data at rest" and "provisions for secure electronic messaging between patients and physicians". In summary, MU requirements mean hospitals/providers must assess their privacy and security practices and make improvements where necessary and appropriate.

Frequently Asked Question

Q: I am conducting a research study with over 50 subjects. I have been granted a waiver or partial waiver and will be completing the Attachment 45 - Accounting For Disclosure(https://www.med.miami.edu/hipaa/private/documents/D3900048E.pdf).Do I need to complete an Attachment 45 for each subject?

A: If you have been granted a waiver/ partial waiver and have over 50 subjects, you may provide an electronic and hard copy spreadsheet. For detailed instructions, please contact the Office of HIPAA Privacy and Security. For questions about IRB protocols, contact Human Subjects Research Office at 305-243-3195.

Have a Question?

hipaaprivacy@med.miami.edu

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

- **HITECH Act:** http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html
- **CMS:** https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html

Protect Paper Records with Sensitive Information

Sensitive information on paper needs to be protected just like sensitive information on a computer. Both need to be protected from unauthorized access or disclosure. Protection of personally identifiable information (PII) and protected health information (PHI), in all forms, is required by various federal and state laws including HIPAA, FERPA and GLBA. PII can also be used for identity theft and other crimes. Examples of sensitive information include names combined with social security numbers (SSN) and/or account numbers as well as health information. Particularly sensitive health information includes HIV status, mental health, substance abuse, STD and reproductive health records.

Recommended safeguards include:

- Printed reports with PII/PHI should identify the individual responsible for printing, date/time and data source.
- Supervisors and managers are responsible for the supervision of employees who have the ability to print such reports. Abnormal printing patterns should be reviewed.
- Avoid printing SSN unless required by law or unavoidable business-related need.
- PII/PHI reports should only be distributed to those with a business/clinical need.

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

PRIVACY & SECURITY NEWS

State Pays $1.7 million for Lost Hard Drive

The State of Alaska announced in June 2012 that it is paying $1.7 million to the federal government for a 2009 security breach of patient data. A federal investigation following the breach found inferior security measures in place at Alaska's Department of Health and Social Services. In October 2009, a portable hard drive was stolen from the car of a computer technician who worked for the State Health department. The investigation that followed found problems with security measures the state was taking to protect patient data. "The security lapses were fairly fundamental and fairly longstanding," Susan McAndrew, Deputy Director for Health Information Privacy with the Department of Health and Human Services, said. She says the settlement amount is high because the list of infractions was so long.

Trial Lawyers: Make a Privacy Mistake, Expect a Lawsuit

MIT's *Technology Review* reports on privacy as "big business for trial lawyers," suggesting "companies that make privacy mistakes can expect a lawsuit." The report features insights from trial lawyers, including one who, in the past eight months, has sued four tech and web giants "alleging that the companies violated U.S. wiretapping laws and committed computer fraud when they tracked users on the web or via their smartphones in ways that broke the companies' own privacy policies." Another attorney points out, "There is a mushrooming number of cases...A decade ago privacy was a distant worry among CEOs and boards of directors, but now it's a full-blown hurricane."

Hospital Pays $750,000 to Settle Alleging Failure to Protect Patient Information

Massachusetts-based South Shore Hospital paid $750,000 to settle a lawsuit alleging that it failed to protect patients' electronic health information (EPHI). The hospital is charged with losing unencrypted backup computer tapes containing EPHI of 800,000 individuals. According to the consent judgment, South Shore Hospital will pay a $250,000 civil penalty and $225,000 toward an education fund that will be used by the Attorney General's Office to promote education concerning the protection of personal information and protected health information. The consent judgment credits South Shore Hospital for the additional $275,000 the hospital spent to beef up its security measures in the aftermath of the data breach. According to Massachusetts AG Martha Coakley, hospitals and other entities that handle personal and protected health information are obligated to properly protect sensitive data, whether it is in paper or electronic form.

Privacy Expert Paul Ohm to Join FTC

Paul Ohm, a law professor/privacy expert at the University of Colorado, is expected to join the Federal Trade Commission as a senior policy adviser focusing on Internet and mobile markets. The appointment signals the agency's continued commitment to bringing privacy and technology related cases. In the past year, the FTC has forged 20-year privacy agreements with Internet giants Google, Facebook and MySpace. Ohm is a former federal computer crimes prosecutor and an expert in information privacy. His 2010 paper, "Broken Promises: Responding to the Surprising Failure of Anonymization" sparked a global reassessment of privacy standards."I am honored to have received this appointment," Professor Ohm said in a press release. "The FTC is the focal point for so many of the important information privacy debates taking place today."

Appeals Court Upholds HIPAA Conviction of EHR Snooper

A federal appeals court has upheld the conviction of a former employee of the UCLA Healthcare System for accessing the hospital's electronic health record system without authorization. Huping Zhou had accessed at least 323 patient records, including those of actors Arnold Schwarzenegger and Tom Hanks, and his boss during a three week period in 2003. Dr Zhou pled guilty in 2010 for violating HIPAA, and was sentenced to four months in prison, assessed a $2,000 fine and a $100 special assessment. Zhou appealed his conviction on the grounds that "he didn't know that it was illegal to obtain the health information". The United States Court of Appeals for the Ninth Circuit affirmed the conviction. The case also may serve as another example of the increased scrutiny of HIPAA compliance and enhanced enforcement environment.

Related Links

- **Protect Paper Records:** http://www.med.miami.edu/hipaa/public/x711.xml
- **State Pays $1.7 million:** http://www.alaskapublic.org/2012/06/26/state-pays-large-settlement-for-patient-privacy-breach/
- **Trial Lawyers:** http://www.technologyreview.com/news/428052/why-privacy-is-big-business-for-trial-lawyers/
- **Hospital pays $750,000:** http://www.informationweek.com/news/healthcare/security-privacy/240001142
- **Privacy Expert:** http://blogs.wsj.com/digits/2012/05/21/privacy-expert-paul-ohm-to-join-ftc-targeting-web-mobile/
- **Appeals court:** http://www.fierceemr.com/story/appeals-court-upholds-hipaa-conviction-ehr-snooper/2012-05-16
- **PII:** http://www.med.miami.edu/hipaa/public/x476.xml
- **PHI:** http://www.med.miami.edu/hipaa/public/x154.xml
- **HIPAA:** http://www.hhs.gov/ocr/privacy/
- **FERPA:** http://www2.ed.gov/policy/gen/reg/ferpa/index.html
- **GLBA:** http://www.ftc.gov/privacy/glbact/glbsub1.htm

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