Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

July 2013 - Issue 26

What's Inside?

Smartphones and Privacy
Random Walkthroughs of UHealth Sites of Service
Privacy & Security News

Smartphones and Privacy

Currently more than half of all American adults use smartphones, according to the Pew Research Center's Internet & American Life Project. Smartphones have features of both a mobile phone and computer, allowing us to talk, text, access email, browse the Internet, take pictures and manage bank accounts. Smartphones can do more and more every day. Unlike our computers, smartphones are ALWAYS with us and many of us rarely turn them off. However, consumers need to be aware of the kind of information that can be collected by various entities from their smartphone.

Service providers (such as AT&T, Sprint, Verizon, and T-Mobile) may be collecting phone numbers called and received, times and duration of calls and your location. Full details of what they are collecting are not clear. In addition to the data collected by your service providers, you should also be aware of possible privacy issues surrounding the collection or disclosures of:

- Photos or video you take with your phone
- Calls, text messages and emails you sent and received on the device
- Websites visited and search terms used
- The contacts you have stored

Who would be interested in the data on your smartphone? Companies, advertisers, cyber-criminals and in some situations, federal agencies would have "an interest" in such data. Apps can collect all sorts of data and transmit it to the app-maker and/or sell it to third-party advertisers. Ads from advertising networks running on some apps may change smartphone settings and take contact and other information without your permission. Some apps may track your location. Location-based services like Google maps, Yelp or Foursquare need your location in order to function properly. However, there are apps that do not need your location to function but may still be tracking it. To read more, including steps to protect your privacy and information, please see http://privacyoffice.med.miami.edu/awareness/tips/smartphones-and-privacy

Frequently Asked Question

Q: Where can I order the Notice of Privacy Practice booklets?

A: If you need to order Notice of Privacy Practice booklets, you may do so in the Ariba Spend Management System (Enet) via Print Farm, the vendor for the current Notice of Privacy Practices.

Have a Question?

hipaaprivacy@med.miami.edu

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

Random Walkthroughs of UHealth Sites of Service

Unannounced walkthroughs are routinely performed at various sites of service of UHealth to review practices that safeguard protected health information (PHI). Some of the elements examined during such walkthroughs include:

1. Computers with access to PHI that are visible to the public, left unattended or unlocked
2. System access passwords inappropriately displayed (e.g., Post-it note stuck on monitor)
3. Patient information left unattended in an unsecure location (e.g., charts left in public area/s)
4. Staff use of approved fax cover sheets when faxing sensitive information
5. Patient information discarded in regular trash cans
6. Sign-in sheets containing more than minimum necessary information (e.g., chief complaint)
7. Phone conversations regarding PHI and/or dictations easily overheard by the public
8. Notice of Privacy Practices prominently posted in patient registration/waiting areas
9. Staff observed wearing name badges
10. Visitors monitored or escorted through restricted areas

A report is prepared outlining the findings, including deficiencies and recommendations for corrective action if applicable. The report is distributed to the site administrator, Vice Chair for Clinical Administration, and/or facility leadership, for follow up as necessary. As always, if you have questions or concerns about this process, please contact the Office of HIPAA Privacy and Security.

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

Patient Privacy, Consent Considerations for Health Big Data

Healthcare organizations are undoubtedly moving toward using large data sets to learn more about patients and become more efficient in patient care. Many are becoming part of health information exchanges or accountable care organizations (ACOs) which further facilitates their big data and predictive analytics efforts. As organizations try to extract value from these massive volumes of patient data, it can be both challenging and convoluted to deal with the related privacy and security issues. At the Institute for Health Technology Transformation Health IT Summit held May 2013 in Boston, an expert panel shared its big data experiences as well as how it sees the industry using the data in the future. Micky Tripathi, CEO of the Massachusetts eHealth Collaborative, spoke about "gray areas" in regards to consent from a state policy and payer perspectives. Chuck Podesta, CIO of Fletcher Allen Heathcare, raised an interesting point about the interactions, especially regarding data security between large and small organizations that are part of an ACO. Responsibility for privacy and patient consent is a huge consideration for ACOs as they build these enormous data sets.

New Poll Shows Americans Anxious About Privacy

Big Brother is watching and Americans know it. New figures from the quarterly Allstate/National Journal Monitor Poll show that most Americans exhibit a healthy amount of skepticism and resignation about data collection and surveillance, and show varying degrees of trust in institutions to responsibly use their personal information. Recent headlines focusing on government collection of telephone records within the United States may further stoke the underlying worries that the American public has about data privacy. With respect to privacy in the future, nine in ten poll respondents said they feel that they have less privacy than previous generations. A clear majority (88 percent) favors a federal policy to require the deletion of online information and nearly four in ten (37 percent) report they have personally experienced fraudulent use of their personal information to make purchases without their consent.

Professor Re-Identifies DNA Study Volunteers

Working with her research assistant and two students, Harvard Data Privacy Lab Director, Prof. Latanya Sweeney, scraped data on anonymous volunteers who shared their DNA with the Personal Genome Project, re-identifying more than 40 percent of the sample, *Forbes* reports. Profiles of anonymous participants include information on medical conditions, illegal drug use, alcoholism, depression, sexually transmitted disease and medications, as well as DNA sequences, the report states, noting Sweeney's team was able to discern identity from ZIP code, date of birth and gender "combined with information from voter rolls or other public records." Sweeney has set up a website to help individuals determine how easily they could be identified by entering those three pieces of information.

Hotel Data Security Issues on the Rise

Chicago Tribune reports on data security issues within the hospitality industry and the alleged rise in identity thefts and malware attacks. One attorney specializing in hospitality law said, "Data security is becoming an issue of significant importance in the hospitality industry." Hackers now attack hotel systems and data in third-party reservation systems not only for credit card data but for additional personal information, including address, license plate number and date of birth, all of which aid in identity theft, the report states.

HHS Issues First Ever HIPAA Fine to Small Organization

The not-for-profit Hospice of North Idaho was fined $50,000 for a breach of protected health information for fewer than 500 individuals under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The fine resulted from an incident involving an unencrypted laptop with patient information that was stolen from the hospice. A federal official said that covered entities, regardless of size, will be held accountable for safeguarding patients' health information. The hospice has entered into a two-year corrective action plan as part of the settlement with the HHS Office of Civil Rights.

Related Links

- **Patient Privacy, consent considerations for health big data:** http://healthitsecurity.com/2013/05/07/considering-patient-privacy-consent-for-healthcare-big-data/
- **New Polls Show Americans Anxious About Privacy:** http://www.darkreading.com/privacy/the-allstate-corporation-new-poll-shows/240156657
- **Re-Identifies DNA Study Volunteers:** http://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/
- **Hotel Data Security Issues on the Rise:** http://articles.chicagotribune.com/2013-04-02/lifestyle/sns-201304020000--tms--traveltrctntt-b20130402-20130402_1_credit-card-reason-hotel-guests-chain-hotel
- **HHS Issues First Ever HIPAA Fine to Small Organization:** http://www.mcknights.com/hhs-issues-first-ever-hipaa-fine-to-small-organization-for-portable-device-data-breach/article/274919/#

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