Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

April 2014 - Issue 28

What's Inside?

The Internet of Things and Privacy

Most people access and share information by connecting to the internet via a computer, tablet, or smartphone. Many willingly share information via FaceBook, Twitter, LinkedIn, Google +, Instagram and Pinterest. There is also a certain, uneasy understanding between consumers and these sites about the terms of use. However, as technology continues its advance, numerous, new devices are also capable of accessing the Internet and transmitting data. This "Internet of Things" can be thought of as a collection of "smart devices" that continuously collect and transmit data via the Internet, without the need for any active human action. This data is continuously being uploaded to the cloud to augment the already enormous amounts of data already collected about every individual on the grid. These internet-enabled smart devices use sensors that can measure and transmit information about location, temperature, speed, or even vital signs such as blood pressure, pulse rate and blood sugar levels.

The Internet can be thought of as evolving into an "always on" tool of surveillance. Some examples of these smart devices include:

- Wearable devices with ability to record events (Google Glasses, Fitbit, Nike Fuel band)
- Medical devices that continuously monitor blood pressure and other vital signs (Infusion Pumps, Cardiac Holters)
- Home security devices (Surveillance Cameras, Baby Monitors)

Frequently Asked Question

Q: Does the University have an authorized vendor for off-site storage of records?

A: The authorized off-site storage vendor for University records is Iron Mountain.

Please visit http://www.miami.edu/finance/index.php/spend_management_and_records_retention/contact_spend_management/ or contact records.management@miami.edu for additional information.

Have a Question?

hipaaprivacy@med.miami.edu

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

While these smart devices have the potential to save time and energy and improve safety and health, the benefits come with significant privacy and security risks. The data collection and potential sharing of that information with others are significant concerns. Even tiny amounts of collected data can, in the aggregate, reveal a great deal about our personal lives. Medical information could be mined and used inappropriately, pricing might be adjusted in a discriminatory manner, and advertisements might be targeted based upon analysis of collected data. To read the complete tip please visit http://privacyoffice.med.miami.edu/awareness/tips/the-internet-of-things-and-privacy.

HHS Publishes Framework for Health IT

On April 1, 2014 the US Department of Health & Human Services published a proposed strategy for a health IT risk-based framework mandated by the Food and Drug Administration and Innovation Act. The draft report identifies three categories of health IT: administrative health IT functions; health management health IT functions; and medical device health IT functions. Risk and corresponding controls should focus on functionality and not on platforms.

There are four areas prioritized in the report:

- The use of quality management principles
- Development and adoption of standards and best practices
- Conformity assessment tools
- An environment focused on learning and continual improvement

The National Coordinator for Health IT Karen DeSalvo said: "ONC welcomes comments on the draft report and stands ready to collaborate with stakeholders to ensure that health IT is designed and used with both innovation and patient safety in mind."

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

FTC's Brill Pushes for Data Privacy Laws

Federal Trade Commissioner Julie Brill has called on Congress to pass three privacy laws, including transparency requirements for data brokers, The Hill reports. Consumers should have the right to view and correct information compiled about them, she said. “I believe we should be concerned about the damage that is done to our sense of privacy and autonomy in a society in which information about some of the most sensitive aspects of our lives is available for analysts to examine without our knowledge or consent and for anyone to buy if they are willing to pay the going price,” Brill said, adding, “I think it is increasingly clear that the United States needs data security legislation.”

Hacker Blackmail leads to Fine for Pregnancy Advice Service

The British Pregnancy Advice Service has been fined £200,000 by the Information Commissioner’s Office (ICO) following a malicious hack and blackmailing incident. Though police recovered the data before a hacker could go through with a threat to publish the names, addresses and contact information of women who’d used the service for advice on pregnancy issues, the ICO still chose to fine the charity because it didn’t realize its website was storing the information and it further was not storing the information securely. “Ignorance is no excuse,” said Deputy ICO Commissioner and Director of Data Protection David Smith. “It is especially unforgivable when the organization is handling information as sensitive as that held by the BPAS.”

Two Sites Concede Heartbleed Data Losses

Canada’s tax authority and a British parenting website, have said some of their users’ data has been compromised as a result of the Heartbleed bug. According to PC World, these are the first two admissions stemming from the now infamous OpenSSL security vulnerability that was exposed recently. The Canada Revenue Agency (CRA) blocked online public access to its site last week. “Regrettably, the CRA has been notified … of a malicious breach of taxpayer data that occurred over a six-hour period,” the CRA said. British parenting site Mumsnet assured its more than one million users it “followed all the published steps to protect members’ security … but it seems that the breach occurred prior to that risk becoming known.”

Group Marketers Thrilled with iPhone Update Allowing Persistent Tracking

With Apple’s latest update to the iPhone operating system, marketing apps can now keep tabs on users’ of Bluetooth-based iBeacon app even if the app is closed, and marketers are thrilled with the change, *NPR* reports. “It was the announcement everybody was waiting for,” said industry insider Doug Thompson. But Seattle-based technologist and writer Garrett Cobarr said, “As a privacy researcher, I always get nervous when marketers are celebratory about something.” Users would assume an app wasn’t tracking them if they had turned it off, and the fact their location is now still being tracked would “ surprise most people and perhaps unnerve them.”

Cloud Computing: Attempts To Physically Control Data Make No Sense

“With cloud computing, many fear losing control. True, supply chains may be complex: services may be layered; separation of ownership, control and use is common” writes cloud computing expert Kuan Hon. Using examples of the evolution of the EU Data Protection Directive, cases from the EU Court of Justice and the Danish Data Protection Agency, Hon outlines reasons the data export restriction and the “transfer to a third country” provisions are antiquated in today’s technological environment. “Nowadays, physically confining data to the EEA does not equate to or guarantee data protection. Yet vast amounts of time and resources are poured into compliance with the restriction, which could be better spent on improving information security.” The fact that “transfer to a third country” is undefined poses another problem. What does “transfer” mean in the internet age?

Related Links

- **FTC’s Brill Pushes for Data Privacy Laws:** http://click.iapp-email.com/?qs=436835c15d4449dd7bf949b1c734194af27926d93ea6d1603093d957c147dd4a
- **Hacker Blackmail Leads to Fine for Pregnancy Advice Service:** http://ico.org.uk/news/latest_news/2014/british-pregnancy-advice-service-fined-200000-07032014
- **To Sites Concede Heartbleed Data Losses:** http://www.pcworld.com/article/2143340/first-sites-admit-data-loss-through-heartbleed-attacks.html
- **Group Marketers Thrilled with iPhone Update Allowing Persistent Tracking:** http://www.npr.org/blogs/alltechconsidered/2014/04/15/302990800/apple-upgrade-tracks-customers-even-when-marketing-apps-are-off
- **Cloud Computing: Attempts To Physically Control Data Make No Sense:** https://www.privacyassociation.org/privacy_tracker

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