CapSpecialty℠
A Community of Insurance Specialists

ARTICLE

Could a Data Breach be Lurking in Your Copier Room?

As if you don't have enough to worry about, now you have to worry about your photocopier. A $1.2 million settlement with the U.S. Department of Health and Human Services (HHS) by a New York not-for-profit managed care plan, in August 2013, was the result of a failure to delete protected health information from a leased photocopier before returning it to the leasing company. Affinity Health Plan, Inc. filed a breach report with HHS after being notified by a representative of CBS Evening News that, as part of an investigative report, CBS purchased photocopiers that had been returned to a leasing company, including from Affinity. The copier used by Affinity was analyzed for CBS and electronic protected health information (ePHI) was found on the hard drive. In fact, the protected health information of over 340,000 individuals may have been compromised. Further, HHS' investigation found that Affinity "failed to incorporate the electronic protected health information (ePHI) stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents".

We live in an age of "smart" devices and machines that are indispensable in our businesses, organizations and private lives. These devices are capable of creating, receiving, maintaining, processing and storing enormous amounts of data. Much of this is "sensitive" data requiring protection under best business practices and various state and federal laws, such as state breach laws and the HIPAA Privacy and Security Rules (for Covered Entities and Business Associates as defined by HIPAA). The risks, as well as the benefits, of these devices must be understood and managed.

There are lessons to be learned from the facts of this case about what your business or organization should be doing to protect sensitive consumer/client information that resides on electronic systems and devices (e.g., social security numbers, credit card numbers, financial information, ePHI, financial information, etc.) and the cost of not doing so, in terms of reputation, liability, business disruption and costs.

First, have a process in place to identify everywhere sensitive data resides on electronic devices, carefully analyze the threats and vulnerabilities to that data and operationalize appropriate safeguards to protect it. That may be easy to say in one sentence but actually doing it can take significant time and resources, depending on the size of the organization, the type and amount of electronic equipment and the type/magnitude of data involved. (See "Resources" below)

Secondly, it's important to understand that this is not a "one time thing". Ongoing risk analysis and updated safeguards are essential because, among other things, technology changes, new devices are added to businesses, ePHI and sensitive information shows up in unexpected places, and employees must be trained on keeping up with the required protections. For example, it's not just copiers, faxes and scanners where electronic information may be found. What about laptops, smart phones, tablets, flash drives, and medical devices that store patient information? The list goes on, as should the analysis and the planning to protect from any breach of information. Hopefully, once that first step is accomplished the ongoing process will not be so overwhelming.

Thirdly, develop and document policies and procedures for risk analysis and for implementing the plan to protect sensitive information. Hint: make sure that one of your policies states "that all personal information is wiped from hardware before it's recycled, thrown away or sent back to a leasing agent". Documentation of policies and procedures communicates the plan internally and externally. Adequate documentation will demonstrate diligence if there is ever a question about whether best efforts were directed at risk analysis, developing policies and procedures, providing employee training, and other activities related to safeguarding individuals' data.

Below are resources about safeguarding sensitive information.

Resources

Federal Trade Commission "Copier Data Security: A Guide for Businesses"
http://business.ftc.gov/documents/bus43-copier-data-security

National Institute of Standards and Technology "Guidelines for Media Sanitation"
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

For Covered Entities and Business Associates per HIPAA

HHS' Office of Civil Rights provides free training about compliance with the HIPAA Privacy and Security Rules
www.hhs.gov/ocr/privacy/hipaa/understanding/training/index.html

Understanding HIPAA Privacy for Covered Entities and Business Associates
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

HHS' guidance on risk analysis requirements under the Security Rule
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
http://www.healthit.gov/providers-professionals/security-risk-assessment

HHS' information about ePHI on mobile devices
www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security