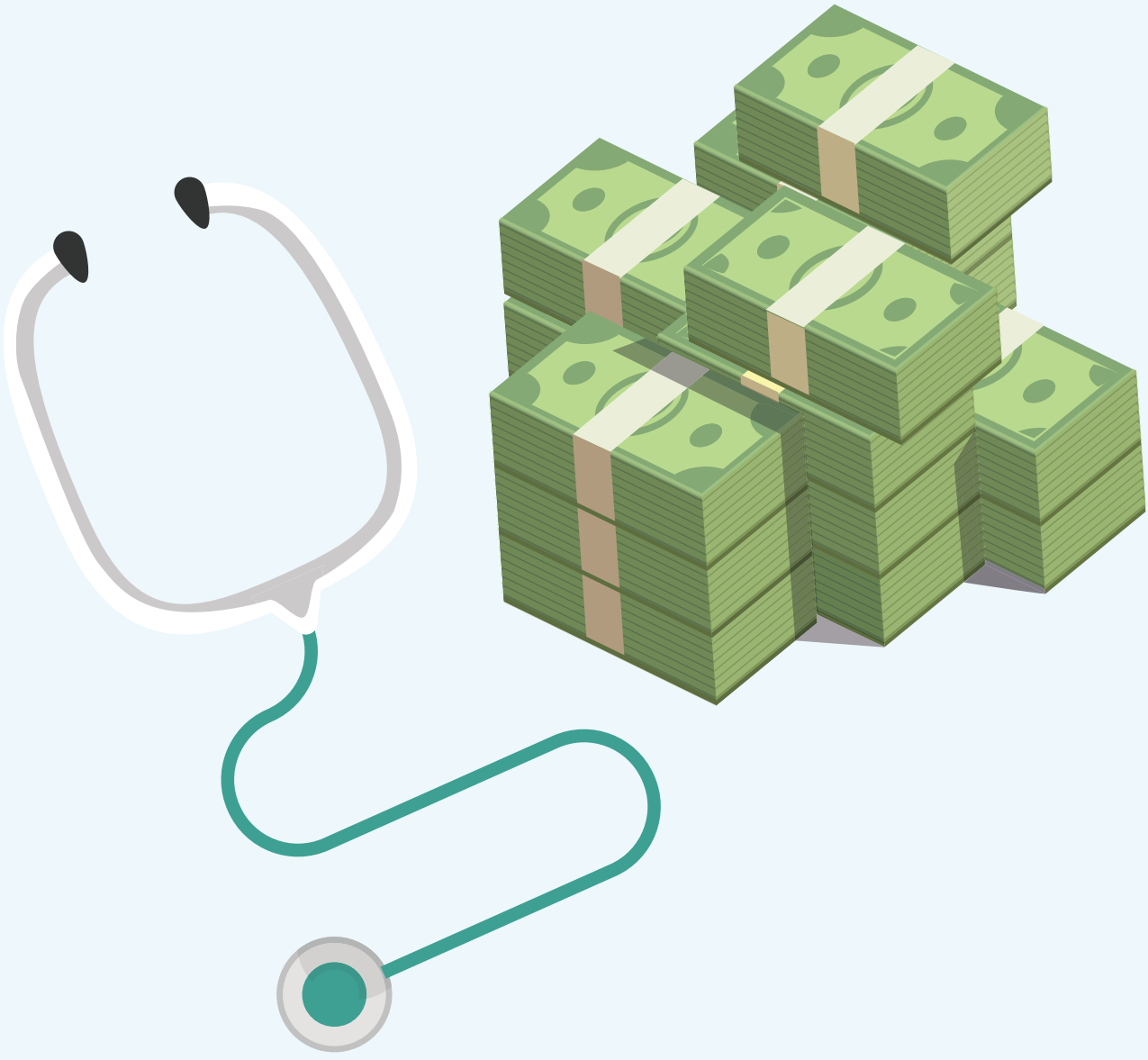
HIPAA Violations Incur Multi-Million Dollar Penalties



ABSOLUTE

Whitepaper

HIPAA Violations Incur Multi-Million Dollar Penalties

Have you noticed how many expensive Health Insurance Portability and Accountability Act (HIPAA) violations have been making the news recently?

In February, 2011, the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) imposed its largest civil penalty to date – a $4.3 million civil penalty against Cignet Health for violations of HIPAA's Privacy Rule.[1]

In July, 2012, the Minnesota Attorney General reached a $2.5 million settlement with Accretive Health, one of the United States' largest collectors of medical debt, for the loss of a laptop containing personal health information (PHI) of approximately 23,500 patients from two hospitals that were customers of Accretive. A condition of the settlement prohibited Accretive from operating in Minnesota for two years.[2]

In March, 2012, Impairment Resources LLC, was forced to file for Chapter 7 bankruptcy when a nighttime burglary resulted in the breach of approximately 14,000 electronic patient records. Rather than face HIPAA violation penalties and civil suits from its customers for privacy breaches, the company simply closed its doors forever.[3]

HIPAA regulations have undergone major changes in the last few years giving both the federal and state Governments new and enhanced powers and resources to pursue HIPAA violations.

WHY HAS THIS HAPPENED?

HIPAA regulations have undergone major changes in the last few years, giving both the federal and state Governments new powers and enhanced resources to pursue HIPAA violations. One of the most empowering aspects of these new regulations is the ability of these Government agencies to use the monies acquired from successful investigations to conduct other investigations.

WHAT CAN I DO IN RESPONSE?

Now, more than ever, the Healthcare industry is under growing pressure to keep personal healthcare information secure to remain compliant with the constantly evolving rules and regulations relating to HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH).

The functionality of Absolute solutions is uniquely suited to help every level of the Healthcare industry maintain compliance and avoid the massive loss in dollars, reputation and staff resources associated with HIPAA-HITECH violations. Absolute provides pre-emptive tools that prevent bad things from happening and reactive tools that can prevent damaging losses from occurring when a security incident unfolds.

The remainder of this whitepaper will give an overview of the evolution of HIPAA-HITECH regulations; why compliance is more important than ever before; and how Absolute can aid in compliance.

A BRIEF OVERVIEW OF THE EVOLUTION OF HIPAA-HITECH REGULATION

HIPAA was enacted in 1996, but was virtually unenforceable for many reasons. HITECH was enacted in 2009 to give teeth to HIPAA's original framework which prevented the unauthorized release of patients' PHI.

HIPAA mandated that regulations regarding the privacy and securing of PHI (typically referred to as the "Privacy Rule"[4] and the "Security Rule"[5]) be promulgated by HHS. HITECH added a requirement that Breach Notification[6] rules should likewise be promulgated. HITECH also provided enforcement resources and enhanced penalties for violations.

Another major phase in this evolution was the HITECH's requirement that an "Omnibus Final Rule" be created by HHS to generate additional regulations to ensure compliance with the Privacy, Secrecy and Breach Notification Rules of HIPAA-HITECH. The Omnibus Final Rule was published on January 25, 2013[7], became effective March 26, 2013, and had to be complied with by September 23, 2013.

WHAT INFORMATION IS PROTECTED?

PHI is any information about a patient's past, present or future mental or physical health or any related billing or payment information that can be connected to a specific patient by any method.[8] The HIPAA-HITECH Privacy Rule and Breach Notification Rule apply to PHI in any form whatsoever, including oral, paper, electronic, etc. The HIPAA-HITECH Security Rule only applies to electronic PHI (ePHI).

The HIPAA-HITECH rules (Privacy, Breach Notification) apply to PHI in any form whatsoever, including oral, paper, electronic, etc. The HIPAA-HITECH Security Rule only applies to electronic PHI (ePHI).

WHO IS REQUIRED TO COMPLY WITH HIPAA-HITECH RULES?

This is one of the significant expansions created by the enactment of the Omnibus Final Rule. HIPAA originally only applied to what is known as "covered entities". Covered entities are front-line providers of medical services: all healthcare providers (doctors, dentists, hospitals, clinics, etc.), health plan employees, clearinghouses, etc. It became readily apparent that covered entities were attempting to avoid HIPAA-HITECH compliance by outsourcing as many services as possible. As a result, one of the expansions brought about by HITECH and the Omnibus Final Rule not only makes business associates of covered entities and subcontractors of business associates required to comply, it also makes covered entities responsible for compliance by those business associates and subcontractors in its downstream. In other words, a covered entity can be held responsible for HIPAA-HITECH violations committed by itself and anyone in its downstream.[9]

A business associate is an entity or person who creates, maintains, receives or transmits PHI. A covered entity can actually be a business associate of another covered entity. A business associate's functions can include "claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefits management; practice management; and repricing" and its services can be "legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial."[10]

WHEN DOES A HIPAA-HITECH VIOLATION OCCUR?

A violation occurs when PHI is released in an unauthorized manner by a covered entity, a business associate or the subcontractor of a business associate. One form of authorized release is when the patient has given knowing consent to the PHI's release. PHI can also be validly released without consent if the release pertains to the patient's treatment, payment of fees or for the normal operation of the enterprise in question. Any other release of PHI is unauthorized.

INCREASED ENFORCEMENT

Prior to the HITECH Act, HHS had to rely solely on submitted complaints to become aware of HIPAA violations. The HITECH Act, and the Omnibus Final Rule which followed, have dramatically increased the likelihood that unauthorized PHI releases will be discovered, for a variety of reasons.

Firstly, the HITECH Act empowered certain federal and state agencies to pursue investigations. On the federal side, OCR was given the authority to investigate complaints and conduct random audits. HITECH also granted jurisdiction to all State Attorneys General to pursue HIPAA-HITECH investigations.

Secondly, HITECH further upset the applecart by changing who bears the onus of identifying PHI breaches. They imposed a breach notification requirement to OCR for any unauthorized release of PHI.

Thirdly, the Omnibus Final Rule increased the likelihood of enforcement actions for HIPAA-HITECH violations by permitting HHS to develop regulations providing for the distribution of collected monies obtained from successful investigation to complainants, offering the means to reward whistleblowers for information provided to OCR.

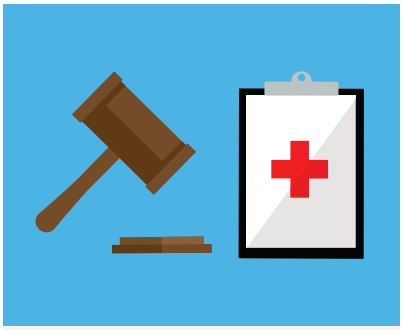
Furthermore, the Omnibus Final Rule has made it easier to enforce HIPAA's Privacy Rule and Security Rule by changing the burden of proof when a breach occurs. Previously, once a breach occurred, the violating entity could simply allege no harm resulted from the breach and it would be up to the complainant to prove harm existed. The Omnibus Final Rule has reversed that, and now, once a breach occurs, it is up to the violating entity to disprove harm occurred.

Finally, OCR completed its pilot program of 115 random audits of covered entities, business associates and their subcontractors at the end of 2012.

The HITECH Act, and the Omnibus Final Rule which followed, have dramatically increased the likelihood that unauthorized PHI releases will be discovered, for a variety of reasons.

INCREASED PENALTIES AND CONSEQUENCES

Under HIPAA, the maximum civil penalty that could be imposed was $25,000 per violation. HITECH increased that to a maximum of $1.5 million. HITECH now also permits HHS to impose fines of a minimum of $100 to a maximum of $50,000 per violation



HITECH also mandated the HHS Secretary to publicly publish the identity of all entities that suffered an unauthorized PHI release affecting at least 500 individuals.[11]

Meanwhile, the legal profession has discovered that there is money to be made by instituting class action lawsuits against entities that have been identified as having their medical records breached. The HH public listing of the breached entities makes them sitting ducks for class action suits. Typically requesting $1000 per affected individual, these suits could become even more destructive than anything HHS or the State Attorneys General can do.

Meanwhile, the legal profession has discovered that there is money to be made by instituting class action lawsuits against entities that have been identified as having their medical records breached. The HH public listing of breached entities makes them sitting ducks for class action suits.

To demonstrate the damage of these suits, below are some examples of recent cases:

- The U.S. Department of Defense is the defendant in a $4.9 billion suit resulting from the theft of a computer backup tape from the car of one of the subcontractor's employees of its business associate. The loss of this tape resulted in the release of PHI for 4.9 million federal employees.[12]
- A north California Healthcare provider was sued for $1 billion for the theft of one of its computers, during a nighttime burglary. containing unsecured PHI of 944,000 patients.[13]
- A Florida health plan provider is the defendant in a class action lawsuit for the theft of two unattended laptops from its headquarters containing PHI of 1.2 million customers.[14]

WHY ENCRYPTION IS NOT ENOUGH

Encryption only works when the person attempting to access the data doesn't have the decryption keys. In fact, the federal Department of Health and Human Services issued a Guidance on April 27, 2009[15], specifically stating that an encryption algorithm is only valid when "the confidential process or key that might enable decryption has not been breached."[16] Documented HIPAA-HITECH violations have occurred involving healthcare provider employees. For example, Huping Zhou, a former UCLA Healthcare System surgeon, was the first person sent to prison[17] for intentionally viewing the PHI of co-workers, supervisors and celebrities after being told he was fired.[18] Dale Munroe, a Florida hospital employee, was sentenced in January, 2013, to a year in prison for accessing medical records of 763,000 patients and selling that information for over $10,000.[19]

Now is the time to act to secure all ePHI in your organization's possession.

PROTECT SENSITIVE HEALTHCARE DATA WITH ABSOLUTE

Now is the time to act to secure all ePHI in the possession of your organization. Every time an entity has a breach of at least 500 patients' unprotected records, the entity's name will be published on a public website, thereby making that entity an easy target for an expensive class action lawsuit.

Absolute provides persistent endpoint security and data risk management solutions for computers, tablets, and smartphones. These solutions provide customers with a unique and trusted layer of security so they can manage mobility while remaining firmly in control. By providing them with a reliable two-way connection with all of their devices, our customers can secure endpoints, assess risk, and respond appropriately to security incidents.

Absolute allows you to respond if a device is missing or stolen, if data is breached or compromised, or if the status of a device is unknown — safeguarding patient data and allowing compliance with regulations such as HITECH/HIPAA and other regional, state, and federal regulations.

FOOTNOTES

[1] http://www.huntonprivacyblog.com/2011/02/articles/hhs-fines-cignet-health-4-3-million-for-violation-of-hipaa-privacy-rule/

[2] http://www.huntonprivacyblog.com/2012/08/articles/minnesota-attorney-general-announces-2-5-million-settlement-with-accretive-health/

[3] http://www.databreaches.net/?p=23593

[4] 45 Code of Federal Regulation (CFR) §164.300 et.sec.

[5] 45 CFR §164.400 et.sec.

[6] 45 CFR §164.500 et.sec.

[7] A copy of the Omnibus Final Rule can be downloaded from http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

[8] HIPAA/HITECH lists 17 specific types of identifiers to connect a patient to his or her medical data, but the 18th category of identifiers is the catchall phrase "any other unique identifying number, characteristic or code." (See 45 CFR §164.514(b)(2)(A-R).) So the 18th category really encompasses not only the first 17 specific identifiers, but any type of patient indentifying information whatsoever.

[9] 45 CFR §164.514(2)(i)(A-R).

[10] 45 CFR §160.103.

[11] Go to http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html/ to see the current list.

[12] http://www.nextgov.com/health/2011/10/class-action-suit-seeks-49-billion-in-damages-from-tricare-data-theft/49929

[13] http://www.simplysecurity.com/2011/11/30/sutter-health-sued-for-1-billion-following-data-breach/

[14] http://www.healthcareitnews.com/news/avmed-health-sued-over-one-largest-medical-breaches-history

[15] See 74 Federal Register 79 beginning at page 19006, available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf

[16] See 74 Federal Register 79 at page 19009.

[17] HIPAA created criminal violations which can be imposed based on the manner and/or purpose of the improper acquisition of PHI with incarceration varying from a maximum of up to one year to a maximum of up to ten years.

[18] http://www.healthcareinfosecurity.com/hipaa-violation-leads-to-prison-term-a-2470

[19] http://articles.orlandosentinel.com/2013-01-14/news/os-hospital-employee-patient-theft-sentence-20130114_1_city-lights-medical-centerdale-munroe-patient-information