THOMSON REUTERS
ACCELUS™

THE HIGH PRICE OF MEDICAL RECORD PRIVACY BREACHES

Melissa D. Berry

The views and opinions expressed in this paper are those of the author and do not necessarily reflect the official policy or position of Thomson Reuters.



THOMSON REUTERS™

ABOUT THE AUTHOR

Melissa D. Berry is a Principal Attorney Editor at Thomson Reuters. Since joining the company in 2000, she has worked on various products, mainly related to insurance compliance, health law, and healthcare compliance. She currently leads the company's Health Policy Tracking Service (HPTS), oversees topic development and writes on Medicaid, the U.S. Food and Drug Administration (FDA), medical malpractice/tort reform and healthcare reform subtopics.

Melissa is a graduate of the University of Akron School of Law and is licensed to practice in Ohio. She is also a member of the American Health Lawyers Association, Association of Insurance Compliance Professionals (AICP) and Public Justice.

INTRODUCTION

In February 2015, Anthem Inc., the second-largest health insurer in the U.S., announced a massive data breach that reportedly resulted in the theft of personal information from an estimated 78.8 million individuals.[1] According to reports, the stolen information included personal details — names, dates of birth, social security numbers, addresses, phone numbers and email addresses but not personal health information.[2]

Community Health Systems, Inc. (CHS) disclosed in August 2014 that its "computer network was the target of an external, criminal cyber attack" in both April and June of the same year. In a Form 8-K filing with the U.S. Securities and Exchange Commission (SEC) in August of that year, CHS stated that a "group originating in China" used malware to access the protected health information (PHI) of approximately 4.5 million individuals who had been referred to or received services from physicians affiliated with the health system.[3]

Security experts are warning health providers and health insurance plans that they may be particularly vulnerable to cyber attacks to obtain personal information that can be sold in the underground markets.[4] Some experts are going so far as to say 2015 will be the "Year of the Healthcare Hack."[5]

Under the Health Information Technology for Economic and Clinical Health (HITEC) Act, a "breach" is the acquisition, access, use or disclosure of PHI in a manner that compromises its security or privacy contrary to the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.[6] Under section 13402(e)(4) of the HITECH Act, the U.S. Department of Health & Human Services (HHS) maintains a website, commonly known as the "Wall of Shame".

When a breach involves 500 or more individuals, the covered entity must notify HHS at the same time it notifies the affected individuals of the breach. This information is then published to the HHS "Wall of Shame," which now includes more than 900 breach notifications.[7] If the breach involves fewer than 500 individuals, the covered entity must notify HHS, but can do so at a later date through an annual report.

For a breach that affects more than 500 residents of a state, in addition to the HHS and affected individuals being notified, the covered entity must also alert "prominent media outlets" in those states.[8]

With 4.5 million affected individuals, the CHS breach was second only to a 2011 data breach of Tricare Management Activity (TMA) that affected 4.9 million individuals. The TMA breach resulted when backup tapes containing PHI were stolen from a car.

---

[1] Caroline Humer, Anthem says at least 8.8 million non-customers could be victims in data hack, Reuters (Feb. 24, 2015) at: http://www.reuters.com/article/2015/02/24/us-anthem-cybersecurity-idUSKBN0LS2CS20150224.

[2] Id.

[3] Community Health Systems SEC Filings, Form 8-K available at: http://www.chs.net/investor-relations/sec-fillings/ (last visited August 30, 2014).

[4] Caroline Humer, Anthem says at least 8.8 million non-customers could be victims in data hack, Reuters (Feb. 24, 2015) at: http://www.reuters.com/article/2015/02/24/us-anthem-cybersecurity-idUSKBN0LS2CS20150224.

[5] Caroline Humer and Jim Finkle, Experts warn 2015 could be 'Year of the Healthcare Hack', Reuters (Feb. 11, 2015) at: http://www.reuters.com/article/2015/02/11/us-usa-healthcare-cybersecurity-analysis-idUSKBN0LF22H20150211.

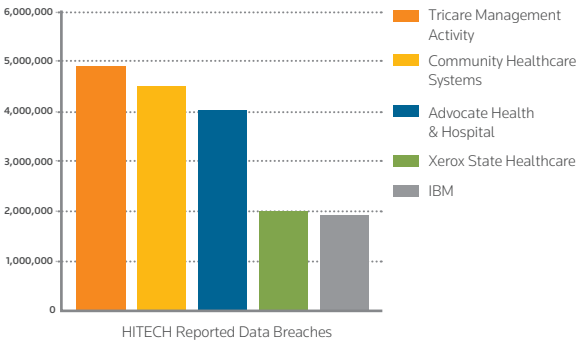
[6] 45 CFR § 164.402

[7] U.S. Department of Health & Human Services Health Information Privacy Breach Tool at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited September 1, 2014).

[8] 45 CFR § 164.406

While breaches of financial information from retailers are often larger and more publicized, healthcare providers, health plans and their business associates must be aware of their breach reporting obligations not only under the HITECH Act, but also under the laws of the state in which they operate.

Top 5 PHI data breaches reported under the HITECH Act[9]



HITECH Reported Data Breaches

FEDERAL REQUIREMENTS

As of September 2013, covered entities, including healthcare providers, health plans, and their business associates, are required to comply with final rulemaking[10] established under the HIPAA of 2016. These rules are aimed at strengthening privacy and security protections, as required by the HITECH Act.

Under the final Breach Notification Rule,[11] covered entities need to notify individuals of a breach of unsecured PHI no later than 60 calendar days following discovery of the breach. Notification can be made by first-class mail or, if the individual agrees to electronic notice, by email. Additionally, if the covered entity does not have adequate contact information for ten or more individuals, it must provide notice through a "conspicuous posting" on its home page for 90 days or a "conspicuous notice" in major media outlets for the geographic areas where the impacted individuals reside.

If the breach notice is delivered, it must include:

1) a brief description of what happened, including the date of the breach and the date of discovery;

2) a description of the types of unsecured PHI involved in the breach;

3) any action individuals should take to protect themselves from potential harm resulting from the breach;

4) a brief description of what the covered entity is doing to investigate the breach, mitigate harm to individuals and protect against further breaches; and

5) contact information of the covered entity to obtain additional information about the breach.[12]

One of the most important changes under the final rule was the removal of the "significant risk" of harm standard in the interim final rule that limited breach notifications. Under the final rule, a breach notification is now required under all situations except those in which the covered entity or business associate "demonstrates there is a low probability that protected health information has been compromised."

---

[9] Compiled from the U.S. Department of Health & Human Services Health Information Privacy Breach Tool at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited February 26, 2015). [7] 45 CFR §§ 164.404 – 164.410.

[10] Available at: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

[11] 45 CFR §§ 164.404 – 164.410.

[12] 45 CFR § 164.404.

The final rule also includes a risk assessment to help the covered entity or business associate determine if a breach notification is necessary. This risk assessment requires consideration of four factors in making this determination:

1) the extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2) the name of the unauthorized person who used the PHI or to whom the disclosure was made;

3) whether the PHI was actually acquired or viewed; and

4) the extent to which the risk to the PHI has been mitigated.[13]

Under HIPAA, PHI includes not only medical or clinical information, but can also include the following:



It is easy to understand the potential risks to individuals due to PHI breaches of this nature and why notification is required.

REPORTED DATA BREACHES AND INVESTIGATIONS

The Office for Civil Rights (OCR) in the Department of Health & Human Services is charged with enforcing the HIPAA privacy and security rules. In addition to receiving notices, the OCR conducts compliance reviews of covered entities and also investigates filed complaints.

In June 2014, the OCR released its Annual Report to Congress on breaches of unsecured protected health information with cumulative data through December 31, 2012.[14] According to its report, the OCR received 236 reports of breaches involving 500 or more individuals in 2011, which affected more than 11.4 million individuals.[15] In 2012, the OCR received 222 reports of breaches involving 500 or more individuals, which affected nearly 3.3 million individuals.[16] Cumulatively, approximately 22.5 million individuals had their unsecured PHI accessed through these larger data breaches.[17] Of course, these numbers now pale in comparison with the recent Anthem and CHS data breaches.

In addition to those larger data breaches, more than 375,000 individuals have had their PHI exposed through smaller data breaches.

---

[13] 45 CFR § 164.402.

[14] Annual Report of Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2011 and 2012 (June 30, 2014) available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreport2011-2012.pdf (last visited September 1, 2014).

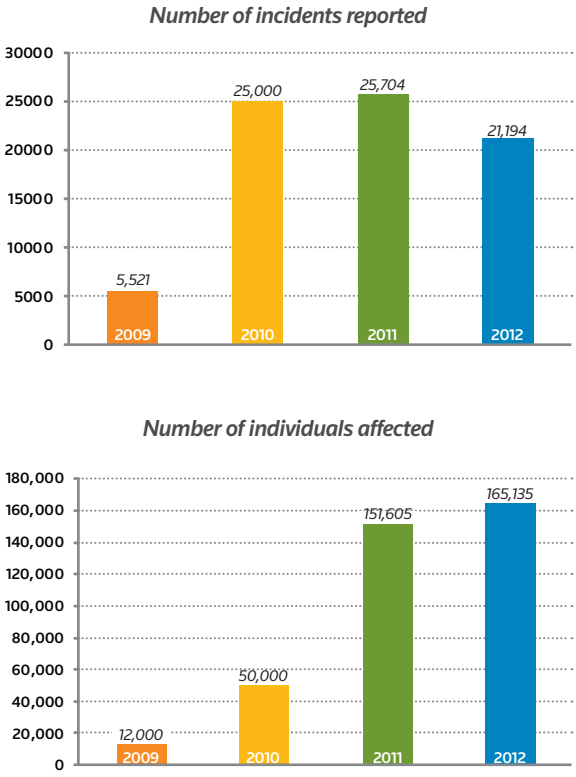
[15] Id. at pp. 4-5.

[16] Id. at p. 5.

[17] Id.

In its report, the OCR also highlighted specific enforcement actions and the resolutions that were reached during the reporting period.

Breaches affecting fewer than 500 individuals



Annual Report of Congress on breaches of unsecured protected health.

Blue Cross Blue Shield of Tennessee (BCBST)

BCBST reported that 57 unencrypted computer hard drives containing the PHI of over 1 million individuals were stolen in 2009 from a leased facility in Tennessee. The information on the hard drives included "member names, social security numbers, diagnosis codes, dates of birth, and health plan identification numbers."[18] The OCR determined that BCBST had not performed the required security evaluation of the leased facility in response to operational changes. It also did not have adequate facility access controls.

Under the resolution agreement with the U.S. HHS in 2012, the first resulting from a HITECH breach report, BCBST agreed to pay $1,500,000 and implement a strong three point corrective action plan (CAP).[19]

Alaska Department of Health and Social Services (Alaska DHSS)

Alaska DHSS reported a breach after "a portable electronic storage device (USB hard drive) possibly containing electronic protected health information (ePHI) was stolen from the vehicle of an Alaska DHSS employee."[20] The OCR reached the decision that Alaska DHSS did not have adequate policies and procedures in place to safeguard ePHI. It also determined that Alaska DHSS had not completed a risk analysis, implemented sufficient risk management measures, finished security training for its workforce, executed device and media controls, or addressed encryption.

Under its resolution agreement with the U.S. HHS in 2012, Alaska DHSS agreed to pay $1,700,000 and implement a five-part CAP.

[18] Id. at p. 20.

[19] Id. at p. 21.

[20] Id.

WellPoint, Inc.

WellPoint reported that the ePHI of over 612,000 individuals was publicly available to unauthorized users over the internet, caused by a weakness in the company's security system.[21] The data "included names, dates of birth, addresses, social security numbers, telephone numbers, and health information."

Under its resolution agreement, in 2013 WellPoint agreed to pay the U.S. HHS $1,700,000. No corrective actions were identified in the OCR Annual Report.

Affinity Health Plan, Inc.

In 2010, Affinity reported the unauthorized disclosure of the ePHI of 344,579 individuals when it neglected to remove the content on the hard drives of leased photocopiers before returning the copiers to a leasing company.[22]

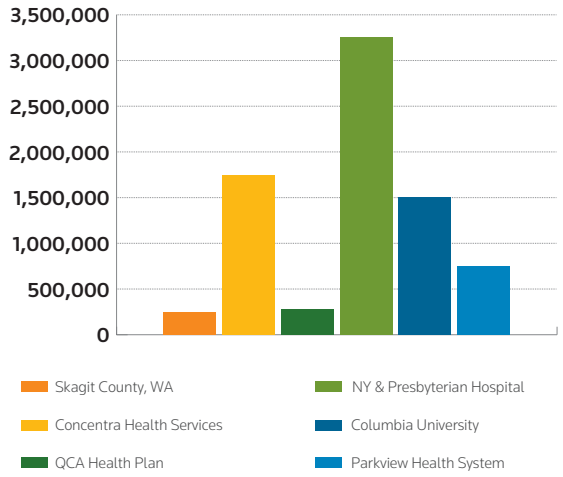
Under its resolution agreement in 2013 with the U.S. HHS, Affinity agreed to pay $1,215,780 and implement a four-step CAP.

FEDERAL PENALTIES

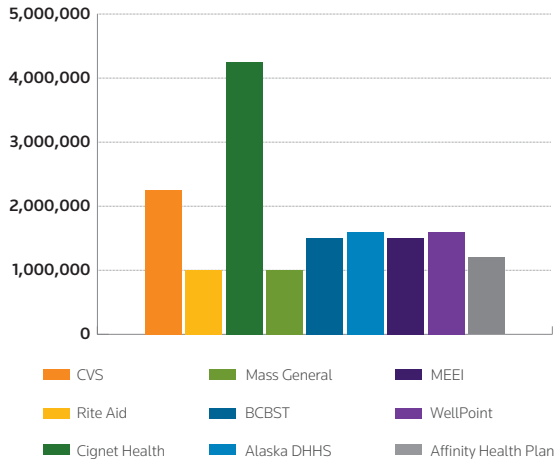
As shown above, in addition to the changes in breach notification requirements, the final rule increased the civil monetary penalties. Penalties were capped at $1,500,000 per violation type, up from $25,000. Depending on the category of the violation, the penalties now range from $100 to $50,000 per violation.

Although the 2014 penalties are high, penalties from 2009-2013 include several penalties of $1,000,000 or more.

2014 reported penalties for HIPAA violations[23]



2009-2013 HIPAA penalties[24]



---

[21] Id. at p. 23.

[22] Id. at p. 24.

[23] Compiled from HHS Case Examples and Resolution Agreements at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/ (last visited September 1, 2014).

[24] Compiled from HHS Case Examples and Resolution Agreements at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/ (last visited September 1, 2014).

STATE ENFORCEMENT

Although the federal government generally takes the lead in investigating these data breaches, the states also have a role in the enforcement of the HIPAA Privacy and Security Rules.

Under the HITECH Act, state attorneys general have the authority to bring civil actions on behalf of state residents when the attorney general "has reason to believe that an interest of one or more of the residents of that state has been or is threatened or adversely affected" by violations of the HIPAA Privacy and Security Rules.[25] The suit may seek to enjoin further violations and/or obtain statutory damages. The statutory damages are calculated by taking the number of violations and multiplying the figure by up to $100. Although the damages are capped at $25,000 per year for "violations of an identical requirement or prohibition," a defendant may also have to pay attorney fees to the state.

Only a few attorneys general have pursued actions under this authority. In 2010, Connecticut Attorney General Richard Blumenthal brought an action against Health Net, Inc. for its six-month delay in notifying nearly 500,000 Connecticut enrollees of the breach.[26] The action was the first of its kind under the HITECH Act. Health Net agreed to pay $250,000 to resolve the claims. Vermont Attorney General William Sorrell also sued Health Net over this data breach, which involved the PHI of 525 Vermont residents. Health Net agreed to pay Vermont a $55,000 penalty and submit to data security audits.[27]

In 2012, Massachusetts Attorney General Martha Coakley settled a lawsuit against South Shore Hospital for $750,000 to resolve HIPAA and consumer protection violations. The suit alleged South Shore Hospital "shipped three boxes containing 473 unencrypted back-up computer tapes with 800,000 individuals' [PHI] off-site to be erased."[28] South Shore Hospital did not inform the off-site vendor that the tapes contained PHI and two of the boxes were lost during shipment.

Attorney General Coakley also settled a smaller PHI disclosure suit in 2013 for $140,000 against a billing practice and four pathology groups relating to allegations that medical records and billing information containing PHI were disposed of at a public dump.[29]

Minnesota Attorney General Lori Swanson filed a suit against Accretive Health, Inc., a debt collection agency, for failing to protect PHI after Accretive lost a laptop containing the unencrypted PHI of about 23,500 Minnesota residents.[30] The lawsuit also alleged violations of Minnesota consumer protection statutes. To settle the allegations, Accretive agreed to pay Minnesota $2,500,000 in 2012. The company also had to cease its operations in the state within 90 days, and could not reenter for a six-year period without the attorney general's authorization.

---

[25] 42 USC 1320d-5(d).

[26] Attorney General Announces Health Net Settlement Involving Massive Security Breach Compromising Private Medical and Financial Info (July 6, 2010) at: http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=462754.

[27] Attorney General Settles Security Breach Allegations Against Health Insurer (January 18, 2011) at: http://ago.vermont.gov/focus/news/attorney-general-settles-security-breach-allegations-against-health-insurer.php.

[28] South Shore Hospital to Pay $750,000 to Settle Data Breach Allegations (May 24, 2012) at: http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-05-24-south-shore-hospital-data-breach-settlement.html.

[29] Former Owners of Medical Billing Practice, Pathology Groups Agree to Pay $140,000 to Settle Claims that Patients' Health Information was Disposed of at Georgetown Dump (January 7, 2013) at: http://www.mass.gov/ago/news-and-updates/press-releases/2013/140k-settlement-over-medical-info-disposed-of-at-dump.html.

[30] Attorney General Swanson Says Accretive Will Cease Operations in the State of Minnesota Under Settlement of Federal Lawsuit (July 31, 2012) at: http://www.ag.state.mn.us/consumer/pressrelease/07312012accretiveceaseoperations.asp.

The attorneys general of Connecticut, Illinois, Massachusetts, Arkansas and North Carolina have already begun investigations of the Anthem data breach.[31] Additionally, the California Department of Insurance will review Anthem's response to the cyber attack.[32]

STATE PHI BREACH STATUTES

In addition to the authority of state attorneys general to enforce federal privacy and security requirements, most states have their own statutes protecting personal information. Although many are general protections, some states have protections that are specific to health information. Only Alabama, New Mexico and South Dakota have no breach notification requirements at this time.

In those states with breach notification requirements expressly including PHI, many incorporate possible substantial civil penalties, administrative penalties or even private causes of action for failure to comply with the breach notification requirements.

For example, in California, "any person or business that conducts business" in that state, and who "owns or licenses computerized data that includes personal information" must disclose any breach "in the most expedient time possible and without reasonable delay."[33] By definition, "personal information" includes medical information and health insurance information.[34] Failure to provide a breach notification can expose the person or business to a "civil action to recover damages" and an award of attorney fees.[35]

In Connecticut, any entity regulated by the Connecticut Insurance Department is required to report any data breach involving personal information to the department no later than 5 days after it has been identified.[36] Depending on the circumstances of the breach, the entity also may be subject to administrative penalties.

In Florida, a recently passed statute replaces the state's prior security of confidential personal information requirements. The new provisions expressly apply to an "individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional" and an "individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual."[37] The statute requires breach notification to Florida residents no later than 30 days following discovery of the breach and sets out the specific notice requirements.[38] A violation of the statute will be treated as an "unfair or deceptive trade practice" and will result in a "civil penalty not to exceed $500,000."[39] However, the statute does not create a private cause of action.[40]

Missouri's breach notification statute also covers health insurance and medical information.[41] The statute sets out the breach

[31] Karen Freifeld, U.S. states probe massive data breach at health insurer Anthem, Reuters (Feb. 5, 2015) at: http://www.reuters.com/article/2015/02/05/anthem-cybersecurity-idUSL1N0VF2LP20150205.

[32] Id.

[33] West's Ann. Cal. Civ. Code § 1798.82(a).

[34] West's Ann. Cal. Civ. Code § 1798.82(h)(1)(D) & (E).

[35] West's Ann. Cal. Civ. Code § 1798.84.

[36] CT Insurance Commissioner Bulletin No. IC-25 (August 18, 2010).

[37] West's F. S. A. § 501.171(1)(g).

[38] West's F. S. A. § 501.171(4).

[39] West's F. S. A. § 501.171(9).

[40] West's F. S. A. § 501.171(10).

[41] V. A. M. S. 407.1500.

notification requirements, which must be made "without unreasonable delay." The Missouri attorney general has the exclusive authority to bring suit for violations and may seek "actual damages for a willful and knowing violation" as well as a civil penalty, not to exceed $150,000 per breach or series of breaches.

In Texas, the breach notification statute covers information relating to the "physical or mental health condition of the individual," "provision of health care to the individual" or "payment for the provision of health care to the individual."[42] Failure to comply with the breach notification requirements[43] can result in civil penalties of up to $250,000.[44] However, only the Texas attorney general can initiate a suit.

Although these jurisdictions represent some of the more serious financial exposures for healthcare providers, health plans or others handling unsecured PHI, other states may also impose unspecified civil or administrative penalties. Additionally, many jurisdictions include general information in their definitions of confidential personal information, such as names, social security numbers, email or street addresses, phone numbers and birthdates, that may overlap with information in medical or insurance records.

CONCLUSION

As discussed above, there are considerable penalties associated with unauthorized disclosures of PHI. Additionally, covered entities will have the expense of breach notifications, the costs associated with corrective actions, updates of software and other security, as well as exposure to private litigation. Those risks make it imperative that healthcare providers and health plans, as well as their business associates, have a complete understanding of how to protect PHI and how to respond if that data is breached.

---

[42] V. T. C. A., Bus. & C. § 521.002.

[43] V. T. C. A., Bus. & C. § 521.053.

[44] V. T. C. A., Bus. & C. § 521.151.

THOMSON REUTERS ACCELUS™

The Thomson Reuters Governance, Risk & Compliance (GRC) business delivers a comprehensive set of solutions designed to empower audit, risk and compliance professionals, business leaders, and the Boards they serve to reliably achieve business objectives, address uncertainty, and act with integrity.

Thomson Reuters Accelus connects business transactions, strategy and operations to the ever-changing regulatory environment, enabling firms to manage business risk. A comprehensive platform supported by a range of applications and trusted regulatory and risk intelligence data, Accelus brings together market-leading solutions for governance, risk and compliance management, global regulatory intelligence, financial crime, anti-bribery and corruption, enhanced due diligence, training and e-learning, and board of director solutions.

For more information, visit accelus.thomsonreuters.com

THOMSON REUTERS™

© 2015 Thomson Reuters GRC01653/3-15