



Breach Report 2011

Protected Health Information

Table of Contents

Executive Summary.	3
By the Numbers.	4
Discussion of Results.	5
Conclusion and Recommendations	9
Appendix:	
Background on Breach Notification Rule.	12

Executive Summary

A total of 385 breaches of protected health information (PHI) affecting over 19 million records¹ have been reported since the August 2009 interim final breach notification regulation was issued as a part of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Redspin's *2011 Breach Report / Protected Health Information* analyzes the full data set of breaches as reported to the Secretary of Health and Human Services (HHS) since the regulation went into effect. By reviewing each incident individually, collectively, and historically, we've identified some increasing threats and troubling trends.

The purpose of our analysis is to help better inform healthcare IT CIOs and other privacy/security professionals. Ultimately, improvements in healthcare IT security must be measured by the reduction of the number of breach incidents and people impacted. Thus, Redspin also provides specific recommendations for preventive action and corrective measures to reduce the most critical vulnerabilities.

By doing so, we hope to facilitate the accelerated adoption of electronic health records – the foundation for improving the cost efficiency, care delivery, and patient outcomes within the U.S. healthcare industry.

¹ These numbers only include breaches that affected more than 500 individuals. Those that impacted less than 500 must also be reported to the Secretary of Health and Human Services (HHS) but are not made publicly available.

By the Numbers

385	breaches of protected health information (PHI)
19,016,894	patient health records affected
49,396	average # of patient records per breach in 2011, an 80% increase over 2010
59%	of all breaches involved a business associate
39%	occurred on a laptop or other portable device
25%	occurred on a desktop PC or server
60%	resulted from malicious intent (theft, hacking)
97%	increase in total records breached, 2010-2011
76%	increase in records breached involving a business associate, 2010-2011
525%	growth in records breached due to loss 2010-2011
5	the top 5 major incidents resulted in 57% of all patient records breached
20	the top 20 major incidents resulted in 88% of all patient records breached

Discussion of Results

A National Epidemic

Breaches of protected healthcare information to date have been widespread throughout the U.S. At least one large IT data breach incident (involving more than 500 individuals) has been reported in 46 of 50 states, the District of Columbia, and Puerto Rico.

Not surprisingly, the most incidents have occurred in the 5 most populous states – California (42), Texas (33), New York (25), Florida (18), and Illinois (19). However, the number of individuals affected per state has less to do with state populations and more to do with the concentration of PHI on unsecured storage devices. Note the prominence of Virginia and Tennessee among the top states on the chart below.

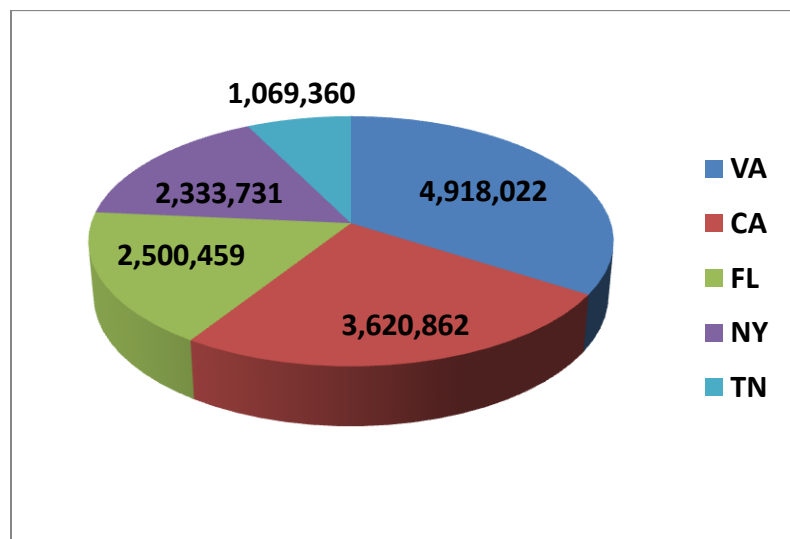


Figure 1: Individuals Affected by PHI Breach by State, Oct 2009 - Nov 2011

Nearly all of the 5 million individual records compromised in Virginia resulted from a single massive breach involving Science Applications International Corporation (SAIC) and Tricare. Data on back-up tapes were stolen from the car of a Tricare employee. Much of the data related to current and retired members of the Armed Services and their families.

Similarly in Tennessee, a single massive breach made up nearly the entire state total. A late 2009 theft of a hard drive at Blue Cross Blue Shield put 1,023,209 patient records at risk.

PHI Breach Incidents – More, More, More

Every day more and more protected health information is reborn in the digital healthcare universe. Often in the form of structured data, ePHI is easier to locate, access, store, transmit, and move. While this offers many benefits, it also presents new risks. Without sufficient controls, one would expect data breaches to become increasingly common over time. Because new records are continually added to existing databases, it is logical to assume that average number of individuals impacted by each new breach would also increase over time.

The 2010-2011 dataset bears this out. During this period, there was a 97% increase in total records breached. Similarly, the average number of patient records per breach increased from 26,968 to 49,394. What could not have been anticipated is the extent to which a few major incidents would dominate the statistics as well as the headlines. The top 20 major incidents caused 88% of all breaches, measured in the number of patients affected. The top 5 incidents (Table 1 below) resulted in 57% of individuals impacted.

Table 1: Top 5 PHI Breach Incidents, Oct 2009 - Nov 2011

COVERED ENTITY	STATE	B/A	DATE	# OF PATIENTS	TYPE	DEVICE/LOCATION
TRICARE	CA	SAIC	9/13/2011	4,901,432	Loss	Backup Tapes
Health Net	CA	IBM	1/21/2011	1,900,000	Unknown	Other
NYC	NY	GRM	12/23/2010	1,700,000	Theft	Electronic Medical Record
AvMed	FL		12/10/2009	1,220,000	Theft	Laptop
Nemours Foundation	FL		8/10/2011	1,055,489	Loss	Backup Tapes

An increasing number of patient records are being put at risk by covered entities and business associates (BAs). Of particular note, the two largest breaches and three of the “top 5” occurred in 2011, further confirmation that the problem is accelerating. It is also incontrovertible that more stringent controls and oversight are needed with regard to business associates. The two largest breaches overall and three of the “top 5” involved a BA.

Lastly, it is strikingly clear that woefully inadequate security risk analysis (if any) took place prior to the occurrence of these incidents. A proper risk-based assessment would have identified and brought attention to these large concentrations of PHI and raised the issue of whether sufficient security controls were in place, either at the covered entity, the business associate, or both.

Guilt by Association

Business associates are third-party vendors, suppliers, consultants, and contractors that covered entities entrust with their PHI to perform services on their behalf. Contractually, BAs commit to having security controls in place to protect the data. However, up until now, ultimate liability for breach remained with the covered entity, at least legislatively. Despite the BA’s contractual commitment to the covered entity, Federal enforcement and penalties have been levied on the covered entity alone, leaving downstream liability of the BA a matter for the courts to decide.

While well intended, this system has not been effective. Since October 2009, breaches of PHI at business associates have made up 59% of all breaches reported. Worse, the current trend is moving in the wrong direction. Total records breached at business associates grew 76% in 2011 as compared to 2010. This has not gone unnoticed by the HHS Office of Civil Rights (OCR). Written into the Interim Final Breach Rule is the provision for civil liability to extend directly to business associates by the end of 2012.

Whether potential civil penalties are enough of a “stick” to make information security a priority at business associates remains to be seen. It does appear inevitable that covered entities will need to take a more proactive role in how BAs protect their PHI.

As part of their regular HIPAA Security Risk Analysis (required under the HIPAA Security Rule and part of the “Meaningful Use” EHR Incentive Program), covered entities should consider the risk exposed to them by their business partners. Some may then decide to require annual IT security audits from high risk BAs as a contractual condition of doing business with them. There may even be some cases where the covered entity will help fund security assessments or improvements. Whatever the result, it has become too big an issue to ignore.

The Media is the Message

A whopping 39% of all PHI breaches to date have occurred on a laptop or other portable media, the easiest type of device for thieves to steal or employees to lose. While stricter policies and more encryption are necessary, both require user training acceptance and enforcement. The problem is likely to get worse before it gets better. Portability is here to stay. Smartphones, iPads, and other tablets are now in use in 80% of healthcare organizations. The BYOD (“bring your own device”) revolution is well underway, yet 50% of respondents in a recent healthcare IT poll say nothing is being done to protect data on those devices.²

Table 2: PHI Data Breach by Source/ Device, Oct 2009 - Nov 2011

Laptop and other portable device	151	39.2%
Paper	92	23.9%
Computer	56	14.5%
Server	38	9.9%
Other	18	4.7%
Email	7	2%
Electronic Health Record	6	1.6%
X-Ray	5	1.3%
Back-up Tapes	4	1%

² Study on Patient Privacy and Data Security, **Ponemon Institute**, December 2011

Hard Drives	3	0.8%
Mail, Postcards	3	0.8%
CD	2	0.5%
Total	385	100%

Back-up tapes deserve a special dishonorable mention. In addition to the Tricare/SAIC disaster, another 1 million+ records were lost on back-up tapes at the Nemours Foundation, a non-profit in Florida dedicated to children’s health.

Risky Business

Several industry estimates have put the value of a stolen health record on the black market at about \$50. Not surprisingly, 60% of all PHI breach incidents have been the result of malicious intent (including hacker attacks, “insider” IT incidents and theft). The previously-referenced *Ponemon Institute Study* reports that 29% of respondents said that PHI breaches at their organization led directly to cases of medical ID theft.

If the data is worth that much to criminals, then it should be worth even more to protect. The cost of a single, large scale breach can be devastating to healthcare companies resulting in organizational disruption, incident response, and brand damage, as well as unplanned expenses ranging from patient and public communications, PR, legal fees, civil penalties, and class-action lawsuit settlements.

Conclusions and Recommendations

The ability to access and share a patient’s health record electronically was a key driver of the HITECH Act. That capability alone has the potential to vastly improve efficiency and patient care, but as the EHR roll-out continues, an unprecedented, nationwide threat to the confidentiality, integrity, and accessibility of protected health information is building. Information security is the Achilles heel of ePHI. Without further protective measures, it could derail widespread implementation and adoption of electronic health records.

Security can only be as strong as its weakest link. Clearly, many business associates are not yet prepared for the responsibility they assume simply by being in possession of PHI. The proliferation of portable devices and media within all IT environments that store PHI increase the likelihood of breach geometrically. Few healthcare employees could tell you what corporate IT security policies are in place; it is even rarer to find security awareness training programs. The number of records breached due to loss of unencrypted devices by employees increased 525% in 2011. It is safe to say that almost no organization knows exactly how to tackle the security implications of the BYOD surge in the workplace.

The solutions won't come from government regulation alone. Incentives and enforcement (civil penalties, Federal HIPAA audits) can play a part, but likely won't (and shouldn't) be prescriptive in sufficient detail. The healthcare industry itself and individual organizations within it must become more proactive in regard to their IT security. In effect, they need to serve as their own watchdog.

A good example is encryption. Of the 385 incidents affecting 500 or more individuals, 55% involved unencrypted devices or media. The Federal government is unlikely to mandate that all portable devices that store ePHI be encrypted, but it's an obvious and sensible policy for a healthcare organization to adopt. Taking it further, why not require that all mobile devices in the healthcare workplace be encrypted, even if ePHI is not allowed on them.

The EHR meaningful use incentives, increased breach penalties and OCR's HIPAA audit program all breathed new life into the HIPAA Security Rule, but that rule was written in 2005. The authors could not have envisioned the explosion in end-points, the ubiquity of wireless access, the threat vectors in web applications, the pervasiveness of social media, and the challenges of BYOD. So we are calling on the Federal government to update the Security Rule so that healthcare providers have more relevant and practical guidance in today's IT environment.

Most covered entities and eligible providers are participating in the meaningful use program. As such, they need to conduct a HIPAA Security Risk Analysis and put a plan

in place to address any vulnerabilities found. Redspin preaches that security assessments are not projects, but rather a part of an ongoing process of durable improvements. As such, we believe SRAs should be conducted on annual or at least bi-annual basis. Healthcare and IT are both dynamic environments. While a comprehensive security assessment has some shelf life, you'll be far more secure if you also assume they have an expiration date.

In regard to business associates, we recommend that hospitals conduct a specific "portfolio" risk analysis as it relates to the dozens or even hundreds of vendors, contractors and consultants they work with. Today, the full legal responsibility of protecting the data remains with the hospital, regardless of "pass-through" contractual provisions. By taking a risk-adjusted approach, the hospital can focus on the subset of BAs that present the greatest potential damage from breach. Ultimately, the hospital has every right to insist that their partners conduct regular, third-party security assessments as a requirement of doing business together.

Lastly, there is no better vaccination against a data breach than improving the security awareness of healthcare workers.

Appendix: Background on Breach Notification Rule

The interim final breach notification regulations,³ issued in August 2009, implement section 13402 of the HITECH Act by requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. If the breach affects over 500 individuals, the covered entity must notify HHS no later than 60 days following the discovery of the breach. Breaches affecting less than 500 individuals need only be reported annually. Business associates responsible for a breach are also required to notify the affected covered entity no later than 60 days following the discovery of the breach.

By definition a breach is generally an impermissible use or disclosure under the Privacy rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

When reporting a breach, the covered entity is requested to provide a variety of information including:

- Dates of breach and discovery
- Number of individuals affected by the breach
- Type of breach
- Location of breached information
- Brief description
- Safeguards in place prior to breach
- Whether or not a business associate is involved

³ <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>

Each breach and associated information listed above was reviewed for this report with the exception of “Safeguards in place prior to breach.” The published data set did not include the safeguard information. In the instances where multiple types and locations were reported, the first type or location has been considered primary in our analysis.