The 2014 Bitglass Healthcare Breach Report

Is Your Data Security Due For a Physical?

BITGLASS REPORT

bitglass

Executive Summary

When Chinese hackers break into U.S. hospital health records to steal patient data, it's a big story. When a laptop is stolen from the local hospital ... not so much. But, according to Bitglass analysis, hacking only accounts for 23% of healthcare data breaches. **Leaving us all to ask, will the real offenders please stand up? Loss or theft of employee mobile devices with information on them—accounts for 68% of all breaches since 2010.**

As part of the Health Insurance Portability and Accountability Act (HIPAA), health organizations must report data breaches that affect more than 500 people. HHS recently made that data available for analysis via its website which it calls "The Wall of Shame", www.hhs.gov. In this report, we take a close look at reported healthcare data breaches over the past three years, and discuss what it means for consumers, healthcare organizations, and the future of digital healthcare records.

23%

Data breaches due to hacking

68%

Data breaches due to loss or theft.

What's really important when it comes to securing health records? Read on and learn the steps healthcare organizations can take now to protect consumers.

The Bitter Truth: You're More Likely to be Robbed than Hacked

Healthcare data breaches affect all sizes and types of healthcare entities, but the overwhelming majority have one thing in common: inadequate security around devices (or paper) containing PHI. According to data from Department of Health and Human Services breach records,

- **A whopping 68% of healthcare data breaches since 2010 occurred when devices or files were lost or stolen, with only 23% due to hacking.**
- **48% of breaches involved a laptop, desktop, or mobile device.**
- **4% of breaches accounted for 80% of total records compromised. Of these 100k record and above mega-breaches, an above-average 78% of compromised records were the result of loss or theft.**

What are these facts teaching us? THIS: Beware of hackers —but pay even closer attention to that employee packing up for the weekend, or taking his/her laptop out the door to his/her car. If healthcare organizations don't start securing the protected health information (PHI) that resides on laptops, desktops, and mobile devices, now then they're bound to lose the data security fight, no matter how hard they fight to protect their data.

What's the Big Deal about Healthcare Data?

HIPAA was passed in 1996 for a very good reason: Medical identity theft can have terrible financial and medical consequences.

◀ A report by the Ponemon Institute calculates the average out-of-pocket loss per victim of medical identity theft at **$18,660**.

For healthcare data breach victims, bad credit, lost insurance coverage, mixed-up records, higher premiums, and the stress of dealing with it are just the beginning. If an identity thief changes patient medical information and a physician diagnoses a problem incorrectly, serious medical harm or even death can result.

In many ways, healthcare data breaches make credit card theft look like child's play. If someone steals your credit card and charges a sky-diving spree, your bank will probably be the first to let you know (and will most likely cancel the charges). Yes, you may be slightly inconvenienced, but rarely does this type of theft result in personal loss.

With PHI breaches, consumers have no such protections. Healthcare organizations, by and large, are not set up to identify illicit records activity and put a stop to it. Healthy patients may not learn about a breach until they have reason to get treatment—probably the worst time to have to deal with such a problem.

But how big an issue is medical identity theft, really?

According to HHS, the total number of breaches per year has remained fairly constant for the past three years—averaging about 200 breaches per year. About 6x as many credit card numbers as medical records are stolen each year. Is PHI theft a growing problem, or is HIPAA doing its job, just as it has been for the past 18 years? In comparison to other industries, healthcare accounts for a whopping 44% of data breaches! HIPAA may be having some impact, but it certainly isn't keeping your local hospital chain from becoming a poster child for stolen personal information.

ANATOMY OF A BREACH

TARGET:	Community Health Services, a Fortune 500 group of 206 hospitals in the U.S.
TIME:	April - June 2014
EXPLOIT:	Heartbleed vulnerability used to steal user credentials and gain network access.
IMPACT:	5.4 Million patient names, addresses, phone numbers, and social security numbers.
COST:	Estimated at $75-$150M in fines, security upgrades and related costs.

4 Reasons why we believe healthcare consumers and providers should be on the alert:

1. **Electronic health records have 50 times the black market value of a credit card.** According to a 2013 EMC report, stolen credit card numbers sell for $1 on the black market, while even a small piece of someone's electronic health record goes for $50. Why? Because you can cancel a credit card—not so with your date of birth, medical diagnosis, or other PHI. Thieves use medical data in many different kinds of fraud and identity theft, and can continue using or selling the information even after the victim knows it's been compromised.

CREDIT CARD NUMBERS GO FOR **$1**

HEALTH RECORDS GO FOR **$50**

2. **Healthcare data is increasingly pervasive.** If you think all your health data is locked up in a hospital database, think again. Today, you can download an iPhone app that can tell if you're depressed. Would you share that information intentionally? Smart devices, such as glucose meters and heart rate monitors, go with you everywhere, uploading your vital details to the cloud in real time. It doesn't take a criminal mind to imagine the implications of such data getting into the wrong hands.

3. **Cloud-based email is on the rise among healthcare organizations.** According to Bitglass' 2014 Cloud Adoption Report, 13% of healthcare organizations now use cloud-based email services, such as Gmail or Microsoft Office 365. While cloud providers generally excel at protecting their infrastructure against attacks, they have no control over what happens to email once it leaves their servers. Is your doctor's assistant sending PHI to her mobile phone? Do employees at your insurance company routinely re-use the same password for all their online applications?

13% OF HEALTHCARE ORGANIZATIONS USE CLOUD EMAIL

4. **90% of healthcare professionals use personal smart phones for work.** Bring-your-own-device (BYOD) is a growing phenomenon, and the healthcare community participates as much as anyone. If a doctor has affiliations with multiple providers, existing solutions, such as Mobile Device Management are out of the question because they require the user to cede control over all applications and data to one organization.

90% OF HEALTHCARE WORKERS USE PERSONAL PHONES

As these factors converge and grow, the threats to healthcare consumers will become increasingly apparent, and with consumer risk comes increased risk for the healthcare organizations that serve them.

The Cost of Data Loss for Healthcare Organizations

Because data breaches are a big deal for healthcare consumers, the cost of breaking the rules is steep: Up to $50,000 per HIPAA violation, or up to $1,500,000 per calendar year per identical violation. In one notable case, an employee of Mass General Hospital absent-mindedly left a file folder on the subway—a mistake that cost Mass General $1 million dollars in fines, since the folder contained the PHI of 192 patients!

$50K
PER HIPAA VIOLATION
OR UP TO
$1.5M
PER IDENTICAL VIOLATION

Lawsuits can be even more expensive, although U.S. judges tend to insist that plaintiffs demonstrate evidence of compensable harm, in addition to increased risk of identity theft. In 2014, most of a $4.9 billion class-action lawsuit involving the U.S. Department of Defense and its TRICARE health insurance program was dismissed for that reason.

The ding on an organization's reputation, is a tough one to recover from one's that trust has been lost. Patients trust healthcare organizations with their most personal and private information, and they expect that information to remain confidential, not end up in the hands of a cyber criminal.

The 5 Essentials For Healthcare Data Security Solutions

Fortunately, healthcare providers have some powerful tools, when it comes to protecting PHI. Today, emerging security technologies, like Cloud Access Security Brokers (CASBs), allow organizations to take a data-centric approach to cloud and mobile security. When you put these solutions into place, you can take device loss or theft out of the equation, and offer true PHI security:

1 **Establish comprehensive IT visibility and control over data transactions.** Emerging technologies known as CASBs , proxy traffic to and from corporate cloud applications and mobile devices, and are essential for any healthcare organization concerned about regulatory compliance and audits. They reverse proxy services are completely transparent to users, and do the heavy lifting of inspecting and securing data, logging activities as they occur, and alerting IT immediately to unusual or unauthorized behavior. Saving IT the headache and man hours.

2 **Control the flow of information**. Securing personal smart phones and tablets is much harder than securing company-managed devices—so take the focus off the devices themselves, and focus on securing the actual data. Today, it's possible to block sensitive information from being downloaded to certain devices, through a set of rules that syntactically and contextually recognize PHI. To maintain HIPAA compliance, your solution must dynamically detect and redact PHI as data flows to BYOD clients.

3

Track and protect sensitive data anywhere it goes. With today's technology, you can place a digital watermark on all sensitive information, allowing you to track the information, see who downloaded it and see what they do with it. When staff members leave the organization, you can selectively wipe corporate data from their personal devices without disturbing any personal data or invading their privacy. Something MDM solutions can't do.

4

Deploy a Single Sign-On (SSO) solution throughout your organization. Know any busy doctors who take pride in their ability to remember 10 or 15 different passwords? Unlikely. SSO solutions deter hackers who may take advantage of common password habits, such as using the same password for different services, or keeping a sticky note underneath the keyboard. They automatically redirect staff to a company login page on the way to accessing any company application. One login—one password. So healthcare workers can focus on saving lives, rather than on logging into the system.

5

Make data security easy to deploy and use. No IT organization has money to burn—healthcare organizations least of all. Cloud applications and mobile devices are ultimately designed to save time and money, so the process of securing them needs to make financial and administrative sense, as well. Any security solution should deploy and scale easily, and with minimal administrative overhead.

In addition, security solutions should always be either invisible to users or built seamlessly into their workflow. Any solution that slows busy healthcare workers down or invades their personal privacy is bound to attract workarounds that defeat security policies. In this business, seconds can mean the difference between saving a life and losing one.

Conclusion

If you look at the HHS Wall of Shame and see your own organization, you're certainly not alone. Even if your name isn't listed for all to see, the likelihood that it could be may be high enough to make you lose sleep at night. But true security for your customers' PHI is not an overly complicated and expensive undertaking.

If you lead an organizations that has avoided the cloud and forbidden BYOD for reasons we've outlined above, it may be time to consider BYOD, now that security technologies have caught up with mobility advancements. We've reached a point where responsible healthcare leaders no longer have to sacrifice staff productivity and morale for the sake of PHI security.

LEARN MORE ABOUT BITGLASS SECURITY SOLUTIONS FOR HEALTHCARE ORGANIZATIONS.

bitglass

About Bitglass

In a world of cloud applications and mobile devices, IT must secure corporate data that resides on third-party servers and travels over third-party networks to employee-owned mobile devices. Existing security technologies are simply not suited to solving this task, since they were developed to secure the corporate network perimeter. The Bitglass Cloud Access Security Broker solution transcends the network perimeter to deliver total data protection for the enterprise—in the cloud, on mobile devices and anywhere on the Internet.

For more information, visit
www.bitglass.com

Phone: (408) 337-0190 | Email: info@bitglass.com