

Breach Report 2010

Protected Health Information



Table of Contents

Executive Summary.1
Findings.2
Background.3
Type of breach.4
Location of breached information6
Business Associates.8
Conclusion9

Executive Summary.

A total of 225 breaches of protected health information affecting 6,067,751 individuals have been recorded since the interim final breach notification regulation was issued in August 2009 as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

However, these numbers only include breaches that affected more than 500 individuals. The number of breaches that affected less than 500 individuals must also be reported to the Secretary of Health and Human Services (HHS) but are not publicly available.

This report reviews the information provided for each publicly-disclosed breach to identify threat trends and recommends which controls will have the greatest impact on reducing the number of incidents in the future.

Findings from the report.

43	states, plus DC and Puerto Rico have suffered at least one breach.
~27,000	individuals, on average, are affected by a single breach.
82 days	on average, pass between breach discovery and notification/update to HHS.
78%	of all records breached are the result of 10 incidents, 5 of which are the result of theft including common storage media, e.g., desktop computer, network server, and portable devices.
61%	of breaches are a result of malicious intent.
~66,000	individuals, on average, are affected by a single breach of portable media.
40%	of records breached involve business associates.

To reduce the likelihood and impact of a future breach, covered entities and business associates should focus their Information Security Programs on the following controls:

1. Implementing encryption on all protected health information in storage and transit.
2. Strengthening information security user awareness and training programs.
3. Implementing a mobile device security policy.
4. Ensuring that business associate due diligence includes a periodic review of implemented controls.

Background.

The Breach Notification Rule of the HITECH Act requires all breaches of protected health information to be reported to HHS. 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 individual¹.”

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

Each breach and associated information listed above was reviewed for this report with the exception of ‘safeguards in place prior to breach.’ The data set available did not include any safeguard information for any breach. In the case where multiple types and locations are associated with the breach, only the first is included in the analysis.

For more information concerning the Breach Notification Rule and to review the original data set, please visit: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>

¹ <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>

Type of breach.

Covered entities are asked to select one or more of the following types of breach: theft, loss, improper disposal, unauthorized access/disclosure, hacking/IT incident, unknown and other. Many incidents selected multiple types indicating a lack of clarity on the definition of each type by the covered entity and perhaps HHS as well.

In an effort to reduce ambiguity, breach types were aggregated into three specific cases based on the description of each incident:

1. A threat-source with malicious intent (theft and hacking/IT incident).
2. A threat-source with unknown intent (loss, unknown, and other).
3. A threat-source with no malicious intent (improper disposal and unauthorized access/disclosure).

61% of all breaches are a result of malicious intent.

Based on this categorization, it is clear that the majority of breaches are a result of malicious intent and result in the majority of records breached (Table 1).

- 62% of total records breached resulted from malicious intent.
- 61% of all breach incidents resulted from malicious intent.
- The highest number of records breached per incident are associated with an unknown intent.

Types of Data Breaches – Threat Source (Table 1)

	Malicious Intent	Unknown Intent	Accident	Total
# Records	3,761,125	1,491,418	815,208	6,067,751
%	62%	25%	13%	
# Incidents	137	35	53	225
%	61%	16%	24%	
# Records/Incident	27,453	42,612	15,381	26,968

Focusing solely on incidents involving malicious intent, it is clear that theft is the leading threat-source, representing 60% of all records breached and 56% of all incidents (Table 2). What is not shown here is loss, which accounts for another 19% of records and 15% of incidents. If one loses something and cannot find it, a likely conclusion is that it has been stolen, thus increasing the probable malicious intent numbers.

Types of Malicious Intent Data Breaches (Table 2)

	Theft	Hacking/IT Incident	All Malicious Intent
# R ecords	3,659,058	102,067	3,761,125
%	60%	2%	62%
# Incidents	127	10	137
%	56%	4%	61%
# R ecords /Incident	28,811	10,207	27,453

It is clear that protected health information is actively targeted and has successfully been compromised by a malicious threat-source.

It is clear that protected health information is actively targeted and has successfully been compromised by a malicious threat-source. This trend will likely increase as Healthcare IT initiatives are deployed across the industry as a result of financial incentives associated with “meaningful use” objectives. It is critical that the necessary security controls are built into each system as it is deployed, not after. The first step is creating a security plan that describes the system, its users and components as well as the security controls that will be relied upon to protect health information.

For better reporting, HHS should consider reviewing the list of breach types from which to select and provide better definitions to avoid overlap and capture consistent information.

Location of breached information.

Covered entities are asked to select one or more of the following locations that contain the breached information: laptop, desktop computer, network server, e-mail, other portable media device, electronic medical record, paper, and other. The category 'Other' included hard drives, backup tapes, and CDs. In addition, many of the 'Other' breaches do not provide additional clarification. Locations were aggregated into three specific cases:

1. Locations that rely on physical controls (desktop computer, network server, e-mail, and electronic medical record).
2. Locations that may or may not rely on physical controls (paper and other).
3. Locations that do not rely on physical controls (laptop and other portable media device).

Based on this categorization, it is clear that locations that cannot rely on physical controls resulted in the highest number of breaches affecting the most individuals (Table 3).

- 65% of all records breached resulted from a laptop or other portable media device.
- 44% of all incidents involved a laptop or other portable media device.
- Twice as many individuals were affected from a portable media breach than a location that can rely on full physical controls.

65% of all records breached resulted from a laptop or other portable media device.

Locations of Data Breaches (Table 3)

	Full Physical Controls	Unknown Physical Controls	Limited Physical Controls	Total
# R ecords	1,294,064	825,678	3,948,009	6,067,751
%	21%	14%	65%	
# Incidents	63	64	98	225
%	28%	28%	44%	
# R ecords/Incident	20,541	12,901	40,286	26,968

Focusing on only portable media breaches, we find that although laptop breaches are more frequent (28% of the incidents), 39% of all records breached are a result of other portable media, including hard drives and backup tapes (Table 4). As a result, over 66,000 records, on average, are breached as a result of other portable media. This means 246% more individuals are impacted as a result of a hard drive, backup tape, or other portable media device breach than an average data breach across all other locations.

Locations of Portable Media Data Breaches (Table 4)

	Laptop	Other Portable Media	All Portable Media
# Records	1,557,913	2,390,096	3,948,009
%	26%	39%	65%
# Incidents	62	36	98
%	28%	16%	44%
# Records/Incident	25,128	66,392	40,286

Devices lacking adequate physical security controls are targeted and successfully compromised more often than devices that utilize available physical controls.

The trend clearly indicates that devices lacking adequate physical security controls are targeted and successfully compromised more often than devices that utilize available physical security controls. However, the use of portable media devices will only increase. Additional controls to consider include disk encryption, strong authentication, remote wipe capabilities, and increased user information security training and awareness. All companies should consider developing their own mobile security device policy, if they haven't already done so.

For better reporting, HHS should consider reviewing the locations from which to select and provide definitions to avoid overlap and capture consistent information.

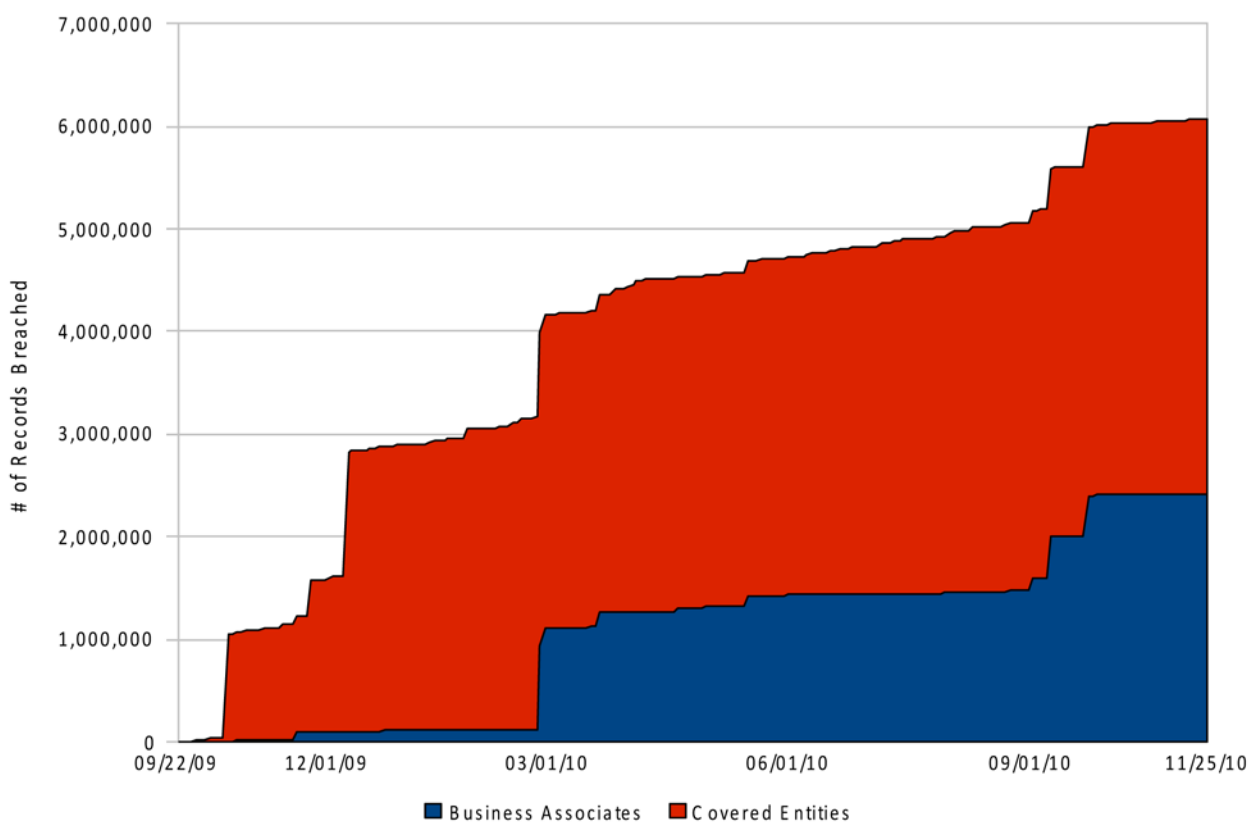
Business Associates.

While business associates have always played a critical role in healthcare IT programs, only after the HITECH Act are they now responsible for implementing the same HIPAA Security Rule safeguards as covered entities, including the responsibility to notify the covered entity if a breach is discovered.

Since breach reporting began in late 2009 business associates are responsible for:

- 4 breaches affecting multiple covered entities.
- Multiple breaches (2 business associates).
- 50 breaches, representing 22% of all incidents of over 500 individuals.
- 2,417,831 total individual records compromised, representing 40% of all breached records (Figure 1).

Breaches Involving Business Associates (Figure 1)



The relatively small number of incidents resulting in a large number of records compromised indicates that business associates are data-rich targets that are likely to see an increase in malicious activity in the future. Despite the varying sizes of business associate IT environments, sufficient resources must be dedicated toward implementing the necessary safeguards as directed by the HIPAA Security Rule.

It is also the responsibility of covered entities to hold their business associates accountable. Aside from typical contractual due diligence, covered entities should ensure business associates prove they have implemented necessary safeguards and those safeguards are working as expected. If a business associate cannot provide the results of an independent security assessment, then consider sending them a self-assessment questionnaire. While it does not replace an objective assessment of the business associates' control environment, the questionnaire will provide the covered entity some visibility into their operations and may provide cause for follow-up investigation.

...business associates are data rich targets that are consequently likely to see an increase in malicious activity.

Conclusion.

This review of published protected health information incidents focused on three areas:

1. The type of breach, including malicious and non-malicious threat-sources.
2. The location of the breach, including portable and non-portable devices.
3. The role of business associates in recent breaches.

By identifying trends in each of these three areas, we hoped to identify a subset of controls that would provide the greatest return on investment to the covered entity and business associate by reducing the likelihood of a successful breach or mitigating the impact of a breach.

Analysis was limited to reviewing only incidents that resulted in 500 or more individual records, which may impact the conclusions. For example, the average number of records breached per incident computed is likely slightly inflated; however, the actual number of breaches and number of records breached are certainly higher than reported here.

To reduce the likelihood and impact of a future breach, covered entities and business associates should focus their Information Security Programs on the following areas:

Incident Detection and Response Implement an incident detection and response program to ensure all incidents are detected and responded to in a timely manner. This includes adequate logging and monitoring systems where protected health information is stored, transferred, and destroyed. Consider developing an incident reporting form that is consistent with the HHS breach notification form. All incidents affecting more than 500 individuals are expected to be reported within 60 days.

System Security Plan During the development of the next IT project and all that follow, whether it be a Blackberry Enterprise Server or an Electronic Medical Record deployment, develop a system security plan that documents each component of the new system, including external connections, where sensitive data is stored, who has access, what vulnerabilities exist with the system, and how to prevent those vulnerabilities from being exploited. Once documented, you now have a roadmap to implement all necessary security controls, test on a regular basis, and monitor to ensure they are always operating as expected. This proactive approach will significantly reduce the ability for a malicious threat-source, whether on the Internet, on the bus, or in the office to successfully steal protected health information.

Portable Media Policy Portable media is here to stay. From tape backups, to laptops, to personal handheld devices, protected health information is on the move. Rather than try to restrict where sensitive information is taken, take a data-driven view and focus on protecting data wherever it is stored. A mobile device security policy that includes management, operational, and technical controls must be defined and implemented. For help getting started, review our Mobile Device Policy Template² which can be customized to your environment. As always, test each control after implementation to ensure it is operating as expected.

Business Associate Oversight Business associates often provide critical IT services and store, process, transmit, and dispose of sensitive protected health information. Ensure your business associate oversight program includes a review of contractual language that requires business associates to take as much care with your protected health information as you do.

2 http://www.redspin.com/resources/whitepapers-datasheets/request_mobile-security-policy.php

In addition, contracts should require business associates to prove on an annual basis that they have adequate safeguards in place surrounding protected health information. If they can not provide the results of an independent security assessment, then consider sending them a self-assessment questionnaire³. While it does not replace an objective third-party assessment of the business associates' control environment, the questionnaire will provide you with some visibility into their operations and may provide cause for follow-up investigation.

While IT environments and threats to these environments are constantly changing, focusing your resources on these four areas will provide an immediate positive impact to your information security program and reduce the risk of a breach of protected health information.



Redspin, Inc.,
6450 Via Real, Suite 3
Carpinteria, CA 93013
800.721.9177
fax 805.684.6859
www.redspin.com

³ http://www.redspin.com/resources/whitepapers-datasheets/request_mobile-security-policy.php