Preventing a Data Breach and Protecting Health Records

One Year Later:

Are You Vulnerable to a Breach?

Kaufman, Rossin & Co.

Table of Contents

Introduction

It was a typical Wednesday afternoon for Jane Smith, the CEO of a large hospital, when she received an alarming phone call from her Information Security Officer (ISO). The ISO informed her that one of their employees had left a laptop case in the open on the back seat of his car. When he finished lunch and returned to his car he found the back window broken and the laptop case missing. Both the laptop and his flash drive were in the case and contained patients' protected health information (PHI). The CEO realized her hospital might be in serious trouble over an incident that easily could've been prevented. Yet she remained calm and ensured that the ISO did the same as she started plotting their next move. "What do we do now?" she asked herself.

On February 17, 2010 the Health Information Technology for Economic and Clinical Health (HITECH) Act was passed, changing the landscape of the healthcare industry dramatically. Incentives, sanctions and penalties regarding non-compliance with the security and privacy of electronic protected health information have been implemented for healthcare providers and their business associates. It's anticipated that there will be a significant amount of electronic health information being exchanged between providers and associates so federal regulations were implemented to improve security and reduce vulnerabilities. There are administrative, physical and technical safeguards that must be in place in every covered entity and business associate.

As of September 23, 2010, there were 166 data breach incidents involving over 500 individuals reported to the Department of Health and Human Services (HHS) and posted on their website. These incidents involved 4,905,768 individuals who had their PHI compromised. The largest of these incidents exposed 1,220,000 individuals in December 2009 resulting from the theft of an unencrypted laptop.

The purpose of this white paper is to review and analyze all of the breaches posted on the HHS website that have occurred between September 23' 2009 and September 23, 2010. We've identified which types of breaches and locations were affected, and highlighted common vulnerabilities and risks. We then offer insight into the best practices for preventing reportable breaches from occurring to help significantly reduce risk of governmental enforcement actions and costs.

Background

2010 has been a pivotal year in the area of healthcare data privacy. September of 2010 marked the end of the first twelve months that breach incidents have been publicly reported to the Secretary of the HHS. In these twelve months, we have also seen the first fines assessed for violations of the new regulations. These events have provided a window into healthcare privacy that had not existed until passage of the HITECH Act.

The HITECH Act

The HITECH Act has established new provisions for the safeguarding of PHI by healthcare organizations (covered entities) and business associates. Organizations required to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), are subject to new regulations for breach notification issued by the HHS. These regulations require covered entities to provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information[1] without unreasonable delay (no later than 60 calendar days.) In the case of a breach at or by a business associate of a covered entity, the business associate is required to notify the covered entity of the breach. If a breach affects 500 or more individuals, the covered entity must notify the HHS, the individuals affected and to the media. Finally, it is required that the Secretary post on an HHS Web site a list of covered entities that experience breaches involving more than 500 individuals. Under the Act, negligent compliance practices can result in fines up to $1.5 million per incident, and each state's Attorney General now has the authority to prosecute organizations that experience breaches.

Breach Notification Rule

Section 13402 of the HITECH Act requires covered entities (CE) and their business associates (BA) to provide notification following a breach of unsecured protected health information. For purposes of determining what constitutes a breach, breach is defined as 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.

There are three exceptions to the definition of "breach" and these are:

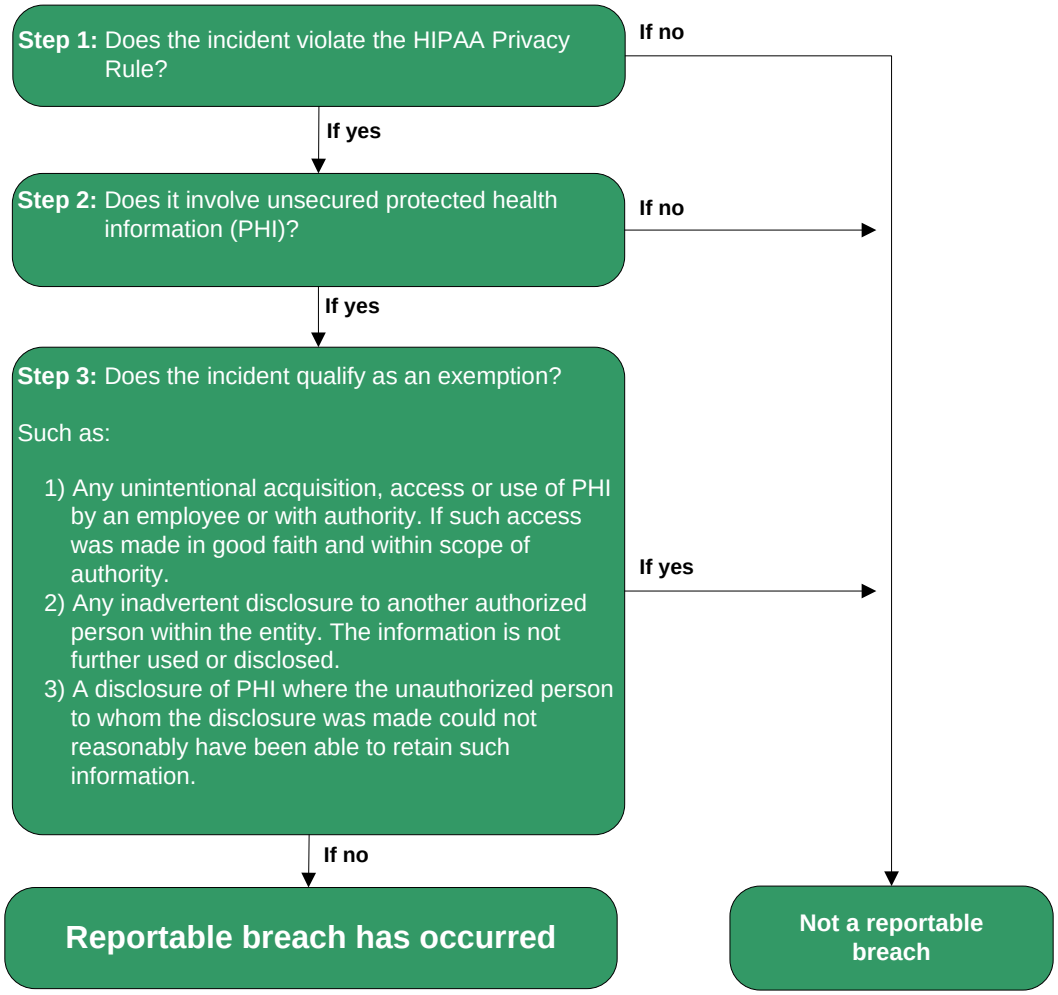
1. **Unintentional acquisition, access, or use by a CE or BA workforce member who was acting in 'good faith' and does not further use or disclose the PHI.**
2. **Any inadvertent disclosure by an authorized person to another authorized person working within the same CE or BA or within an 'organized health care arrangement' which the CE is part of, as long as the PHI inadvertently disclosed is not further used or disclosed.**
3. **Disclosure of PHI where the CE or BA has "a good faith belief" that the unauthorized recipient "would not reasonably have been able to retain such information.**

[1] **Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5 on the HHS website.**

Burden of Proof

CEs and BAs have the burden of proof to demonstrate that (a) a use or disclosure of unsecured protected health information did not constitute a breach or (b) if it constitutes a reportable breach, all required notifications have been provided.

With respect to breach notification, CEs need to comply with several other provisions of the Privacy Rule. The following decision tree, Figure 1, based on the HITECH act Breach Notification Risk Assessment Tool prepared by North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) can be used if a suspected breach[2] that may constitute a reportable breach and will require notification has occurred.



[2] **"Breach" means the acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information. For purposes of this definition, "compromises the security or privacy of the protected health information" means poses a significant risk of financial, reputational, or other harm to the individual.**

Location of Breached Information

PHI can be vulnerable to a breach in any of the recognized data states: data in motion (data moving through a network); data at rest (data that resides in databases, file systems, and other structured storage methods); data in use (data in the process of being created, retrieved, updated, or deleted); or data disposed (discarded paper records or recycled electronic media).

If you are a covered entity or business associate and you have not conducted a protected health inventory to identify where data is stored, transmitted and used you may be exposed to a breach. Figure 18 provides a list of locations that were breached, the type of breach and number of times it was breached in the twelve month period.

Figure 18: Location of Breaches

LOCATION OF BREACH	Theft	Loss	Improper Disposal	Unauthorized Access	Hacking/IT Incident	Other	Unknown	Number of Times the Breach Occurred	Approx. Number Of Individuals Affected
Laptop	•	•		•		•		43	1,503,370
Hard drives	•					•		2	1,082,387
Portable Electronic Device, Electronic Medical Record, Other		•						1	800,000
Other	•	•				•		11	507,477
Portable Electronic Device, Other	•	•				•		11	278,044
Desktop Computer	•		•		•	•		18	228,328
Network Server	•	•		•	•	•		11	166,156
Paper Records	•	•	•	•		•		33	119,806
Postcards				•				1	83,000
Portable Electronic Device	•	•						9	44,015
Mailings				•				2	18,400
Portable Electronic Device, Electronic Medical Record	•							2	17,360
Desktop Computer, Paper Records						•		1	13,000
Backup tapes	•	•						2	12,562
CDs	•							1	5,700

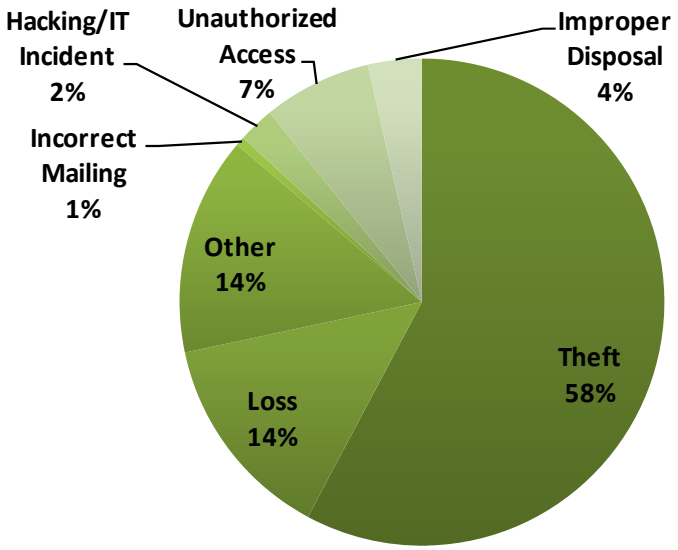
LOCATION OF BREACH	Theft	Loss	Improper Disposal	Unauthorized Access	Hacking/IT Incident	Other	Unknown	Number of Times the Breach Occurred	Approx. Number Of Individuals Affected
Laptop, Desktop Computer, Portable Electronic Device	•							1	4,328
E-mail				•		•		5	3,987
Network Server, Desktop Computer	•							1	3,500
Laptop, Desktop Computer	•							3	3,146
E-mail, Portable Electronic Device	•							1	2,416
Computer, Network Server, Electronic Medical Record					•			1	2,000
Electronic Medical Record				•				1	1,740
Desktop Computer, Other	•							1	1,537
Paper Records and Films	•							1	1,300
Laptop, Desktop Computer, Network Server, E-mail	•							1	1,020
Computer	•							1	689
Desktop Computer, Network Server, Paper Records	•							1	500

LEGEND: • = Location Was Breached

Why Data Breaches Happen

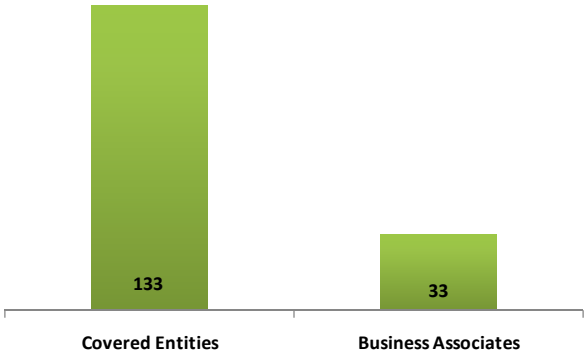
In order to prevent a data breach, it is essential to understand how and why they occur. The HHS website defines seven types of breaches that affect protected health records regardless of the format (paper or electronic): theft, loss, other, incorrect mailing, hacking/it incident, unauthorized access and improper disposal. Figure 2 shows that the primary causes of a data breaches were theft (58%), while other and loss tied in second place (14%).

Figure 2: Number of times the type of breach occurred.



As seen Figure 3, the number of incidents in which business associates were involved totaled 33 (20%) and covered entities totaled 133 (80%).

Figure 3: Number of incidents in which business associates were involved.



According to Figure 4, theft, loss and other affected over 500,000 individuals because of the breach. This graph distributes the type of breach by the number of individuals affected. Theft affected 3,123,800 individuals; loss, 1,038,814 individuals; other, 509,138 individuals; incorrect mailing, 83,000 individuals; hacking/IT incident, 63,610 individuals; and unauthorized access, 53,967 individuals.

Figure 4: Number of individuals affected based on the type of breach.

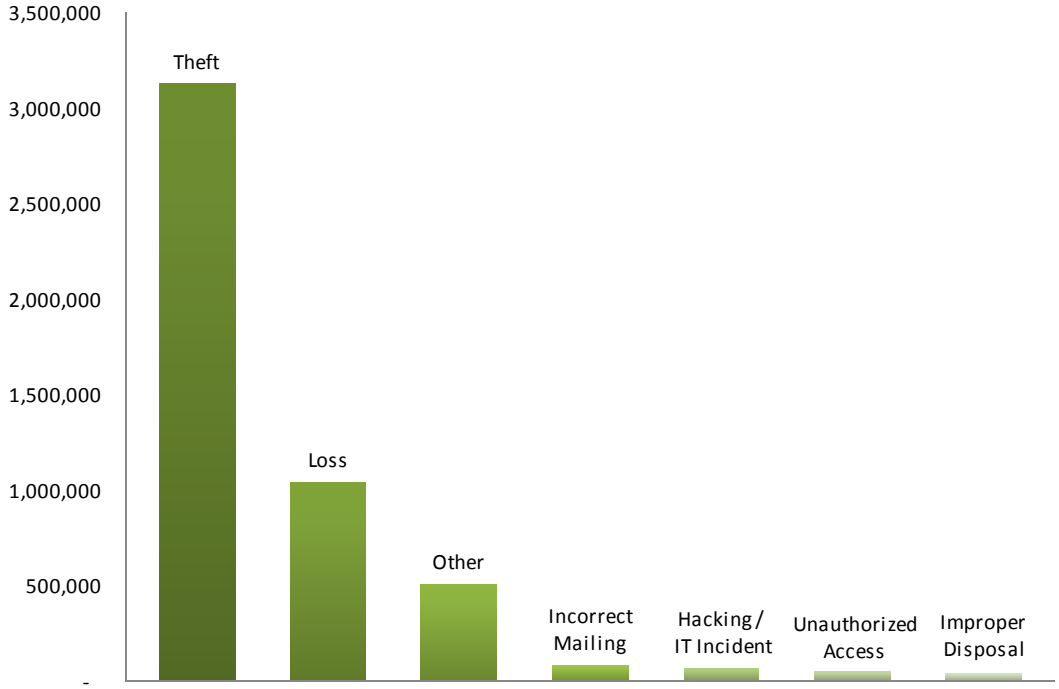
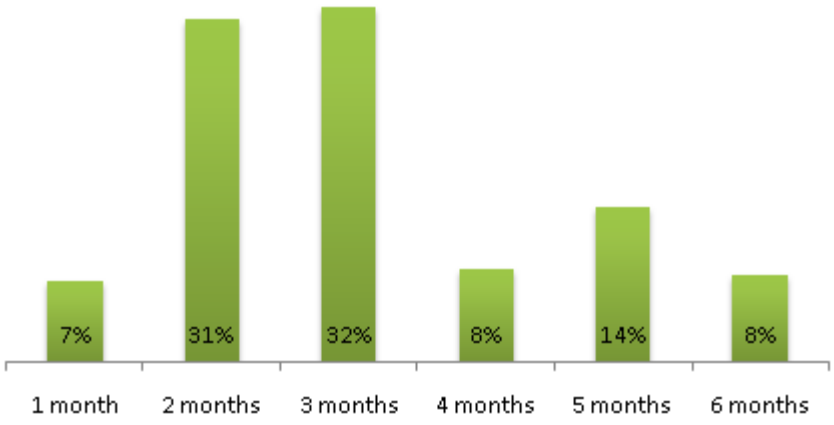


Figure 5 shows that 32% of the breaches that were reported within three months from the date of breach and date it was posted in HHS website. The fastest notification was 6 days and the longest took 276 days.

Figure 5: Average time to notify the HHS from date of breach.



Theft

In order to better understand how breaches happen, below are some examples taken from the HHS website regarding theft.

Impostor posing as a representative of a legitimate vendor
Protected health information was released from the covered entity when an imposter, posing as a representative of the legitimate recycling service used by the covered entity, removed several barrels of purged x-ray films and film jackets. The barrels contained the protected health information of approximately 1,300 individuals.

A laptop computer was stolen from a hospital employee's vehicle
The computer contained the protected health information of 943 individuals. The protected health information involved in the breach included names, contact information, dates of birth, social security numbers, medical record numbers, and health insurance information including diagnosis code in numeric form and billing code description.

A binder with printed protected health information was stolen from an employee's vehicle
The covered entity was unable to determine the number of affected individuals, but the stolen binder contained the information of up to 1,272 patients. The protected health information involved in the breach included names, telephone numbers, detailed notes regarding treatment and possibly the patients' Social Security numbers.

Documents were stolen by an employee
Documents containing protected health information were lost when an employee of the covered entity confiscated and eventually destroyed them. The breach affected approximately 8,000 individuals. The documents contained names and financial information.

Forms were stolen
A covered entity discovered that remittance forms containing member information that accompany paper checks were stolen. The invoices contained the protected health information of over 735 individuals.

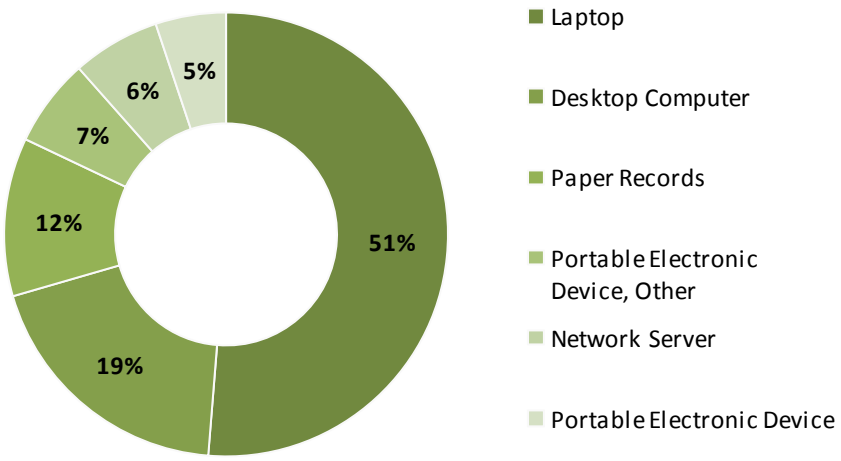
Out of the 166 reported breaches, theft was reported as the type of breach 96 times. 3,123,800 individuals were affected by theft. Figure 6 provides 19 locations of breached information, with the number of individuals affected by the breaches and the number of instances the location was reported.

Figure 6: Locations of breached information and number of individuals affected.

Locations of Breached Information	Number of Individuals Affected	Number of Instances
Laptop	1,496,516	40
Hard Drives	998,442	15
Portable Electronic Device, Other	232,129	9
Desktop Computer	223,596	5
Network Server	74,126	5
Paper Records	18,513	4
Portable Electronic Device, Electronic Medical Record	17,360	3
Portable Electronic Device	13,943	2
Desktop Computer, Other	13,000	2
Backup Tapes	10,000	1
CDs	5,700	1
Laptop, Desktop Computer, Portable Electronic Device	4,328	1
Other	3,576	1
Network Server, Desktop Computer	3,500	1
Laptop, Desktop Computer	3,146	1
E-mail, Portable Electronic Device	2,416	1
Paper Records and Films	1,300	1
Laptop, Desktop Computer, Network Server, E-mail	1,020	1
Computer	689	1
Desktop Computer, Network Server, Paper Records	500	1
Total	3,123,800	96

Figure 7 shows the 6 major locations where information was breached most often (78 times). As shown below laptop (51%), desktop computer (19%) and paper records (12%) were the most commonly stolen, most likely due to their accessibility.

Figure 7: Thefts: Locations storing PHI that were stolen most often.



Loss

Here are examples taken from the HHS website regarding loss.

A business associate mailed a backup tape and CD
A business associate mailed a package to the covered entity that was supposed to contain a backup data tape and compact disc (CD) containing protected health information, but the tape and the CD were not in the package. Approximately 2,000 individuals were affected by the breach. Individual demographic, financial and clinical information was included in the protected health information.

Invoices never located
A month's worth of client invoices went missing; evidence shows that the documents were never mailed, but despite a thorough search, the invoices were never located. The invoices contained the protected health information of over 500 individuals. The protected health information involved in the breach included names, dates of birth, and medical testing information.

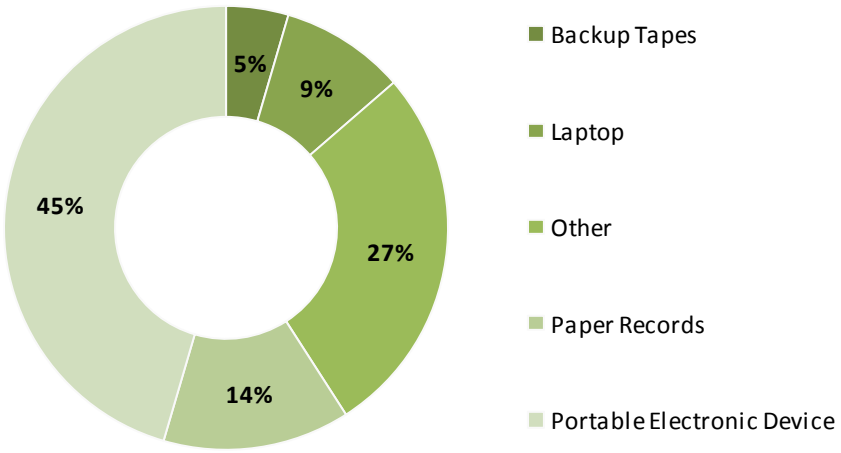
Out of the 166 reported breaches, a total of 22 times was reported for loss as the type of breach. A total of 1,038,814 individuals were affected by loss. For purpose of our analysis we included all loss incidents and a combination of other and improper disposal. Figure 8 provides 7 locations of breached information. Next to each location you will find the number of individuals affected by the breach and the number of instances the location was reported.

Figure 8: Locations of breached information and number of individuals affected because of a lost PHI.

Locations of Breached Information	Number of Individuals Affected	Number of Instances
Backup Tapes	2,562	1
Laptop	5,545	2
Other	158,162	6
Paper Records	8,798	3
Portable Electronic Device	30,072	5
Portable Electronic Device, Electronic Medical Record, Other	800,000	1
Portable Electronic Device, Other	33,675	4
Total	1,038,814	22

Figure 9 shows the 6 locations where information was breached most often (22 times). As shown in below portable electronic devices (45%), other (27%) and paper records (14%) were the most frequently lost, most likely due to their portability.

Figure 9: Losses: Locations storing PHI that were lost most often.



Other

Below are examples taken from the HHS website regarding "other" breaches.

A nurse improperly used information
A nurse used the protected health information of patients to obtain narcotics from the Tomah Memorial Hospital for her own personal use. Tomah Memorial Hospital reported that approximately 600 patients were affected by the breach. The protected health information involved in the breach included the names and account numbers of the patients.

Sending an email
An employee of a business associate sent an email concerning a dietary program to multiple patients without concealing patient email addresses. The names and email addresses were visible to all recipients. The breach affected 937 individuals. In response to this incident, the covered entity took steps to enforce the requirements of its agreement with the business associate.

Social security numbers were printed on the address label
Social security numbers were inadvertently printed on the address labels in a newsletter mailing. The mailing had 560 recipients.

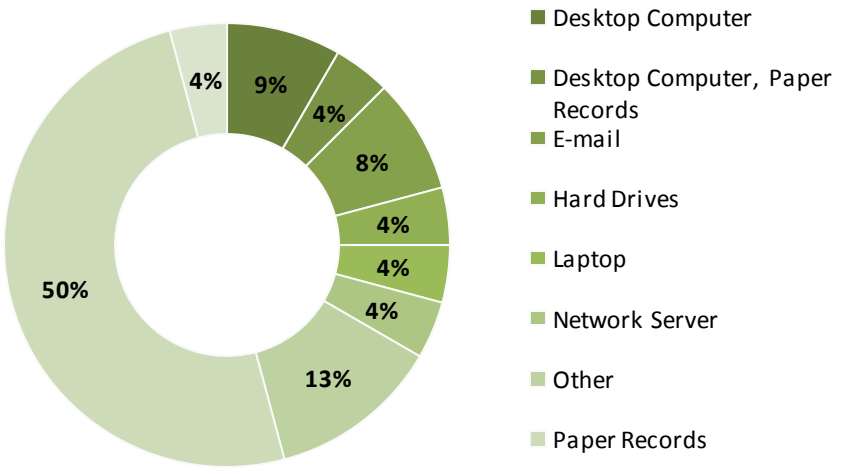
Out of the 166 reported breaches, "other" was reported as the type of breach 24 times. A total of 509,138 individuals were affected. Figure 10 provides 8 locations of breached information, with the number of individuals affected by the breach and the number of instances the location was reported.

Figure 10: Locations of breached information and number of individuals affected because of other.

Locations of Breached Information	Number of Individuals Affected	Number of Instances
Desktop Computer	2,432	2
Desktop Computer, Paper Records	1,537	1
E-mail	1,938	2
Hard Drives	83,945	1
Laptop	1,309	1
Network Server	22,642	1
Other	345,739	3
Paper Records	38,156	12
Total	509,138	24

Figure 11 shows a breakdown of the locations where information was breached most often (24 times). As shown below paper records (50%), other (13%), desktop computer (9%) and email (8%) were the most commonly lost, most likely due to their portability.

Figure 11: Most often locations storing PHI that were considered "other."



Incorrect Mailing

Below are examples of breaches caused by incorrect mailings.

<u>Social security numbers were printed on the address label</u>
The mistake occurred because Social Security numbers are often used as Medicare account numbers. The covered entity responded by firing the business associate responsible for the mailing, and offering one year of free credit monitoring to the Medicare members whose Social Security numbers have been compromised.

Out of the 166 reported breaches, a total of 1 time was reported for incorrect mailing as the type of breach. A total of 83,000 individuals were affected by incorrect mailing.

During our research we noted that two other incidents that were reported by the covered entity and business associate as unauthorized access could have been easily reported under incorrect mailing as the business associate incorrectly emailed the wrong information to the patients.

Figure 12 provides 1 location of breached information due to incorrect mailing, the number of individuals affected by the breach and the number of instances the location was reported.

Figure 12: Locations of breached information and number of individuals affected.

Locations of Breached Information	Number of Individuals Affected	Number of Instances
Postcards	83,000	1
Total	83,000	1

Hacking/IT Incident

Here are examples regarding hacking and IT incidents.

An insurance company hired a computer company to upgrade an internet-based application
An insurance company hired a computer company to upgrade an Internet-based application system and a flaw left open the possibility that people could see others' applications. Information available included names, social security numbers, credit card information, health information and medical history.

File server hacked at a University
A university learned that one of its file servers had been compromised, which potentially exposed the records to an unauthorized source.

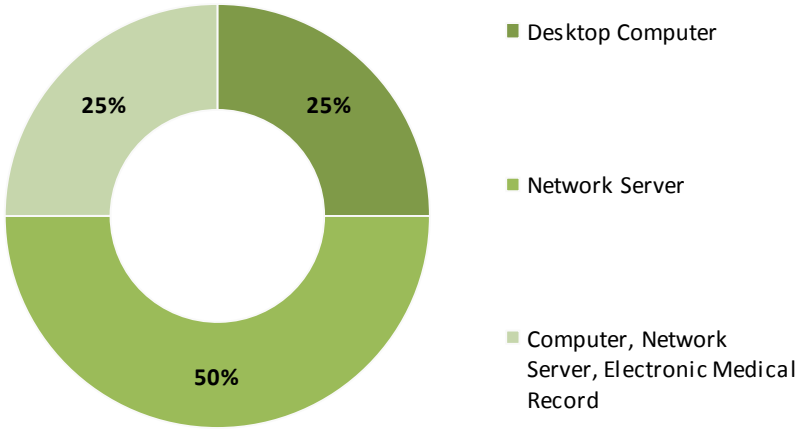
Out of the 166 reported breaches, Hacking/IT Incidents were reported 4 times as the type of breach. A total of 63,000 individuals were affected by this type of breach. Figure 13 provides 3 locations of breached information due to hacking, the number of individuals affected by the breach and the number of instances the location was reported.

Figure 13: Locations of breached information and number of individuals affected.

Locations of Breached Information	Number of Individuals Affected	Number of Instances
Network Server	58,700	1
Desktop Computer	2,300	1
Computer, Network Server, Electronic Medical Record	2,000	2
Total	63,000	4

Figure 14 shows a breakdown of the 3 locations where information was breached most often (4 times) by hacking. As shown below network servers (50%) the most commonly hacked, most likely due to the amount of protected health records stored at the server level.

Figure 14: Locations storing PHI that were hacked most often.



Unauthorized Access

Here are examples regarding unauthorized access.

Filing cabinet inadvertently contained protected health records

Medicare members' information was inadvertently left in a filing cabinet donated with other surplus office furniture to a local nonprofit organization.

Radiologist accessed radiology reports using other's passwords

A covered entity had reason to believe that a radiologist accessed patient radiology reports using the passwords of other radiologists and an employee within the Radiology Department.

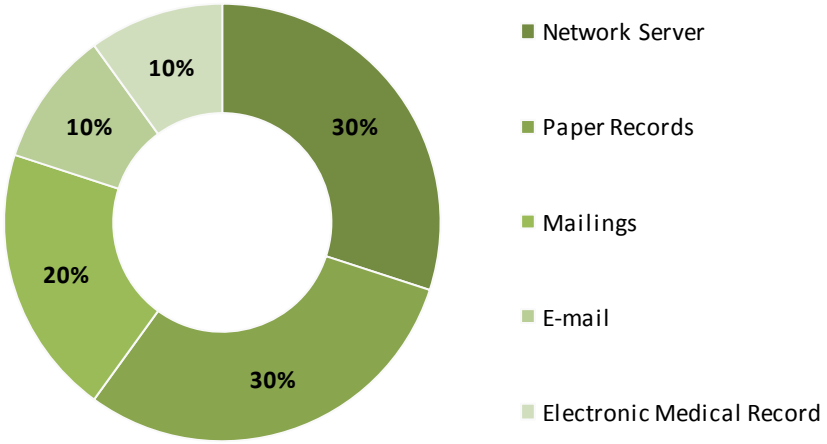
Out of the 166 reported breaches, unauthorized access was reported as the type of breach 10 times. A total of 50,491 individuals were affected by this type of breach. Figure 15 provides 5 locations of breached information, the number of individuals affected by the breach and the number of instances the location was reported.

Figure 15: Locations of breached information and number of individuals affected.

Locations of Breached Information	Number of Individuals Affected	Number of Instances
Paper Records	18,900	3
Network Server	10,688	3
Mailings	18,400	2
E-mail	763	1
Electronic Medical Record	1,740	1
Total	50,491	10

Figure 16 shows a breakdown of the locations where information was breached most often (10 times) by unauthorized access. As shown below network server (30%) and paper records (30%) were the most commonly accessed, most likely due to the amount of protected health records stored at a central location.

Figure 16: Locations storing PHI that were accessed in unauthorized manner most often.



Improper Disposal

Here are examples of improper disposals that led to breaches.

Paper records improperly deposited
Paper records of approximately 24,000 individuals were improperly deposited at a dump.

Out of the 166 reported breaches, improper disposal was reported as the type of breach 6 times. A total of 35,439 individuals were affected by this type of breach. Figure 17 provides 1 location of breached information. Next to each location you will find the number of individuals affected by the breaches and the number of instances the location was reported.

Figure 17: Locations of breached information and number of individuals affected.

Locations of Breached Information	Number of Individuals Affected	Number of Instances
Paper Records	35,439	6
Total	35,439	6

Preventing a Breach

With the HITECT Act, we will see more security breaches reported. Unfortunately, you will always be at risk of a security breach occurring at your organization. However, from the reported breaches we can learn.

Take the following steps to protect your patients' medical information:

- **Review policies and procedures for safeguarding the physical security of your practice. Evaluate whether desktops and network servers are easily accessible.**
- **Encrypt new and existing laptops. If encryption is not feasible, CEs and BAs should evaluate the business need to keep protected health records on laptops or mobile devices. If it is not needed, delete the information.**
- **Retrain all employees on your information security policies and procedures. Focus on policies regarding safeguarding laptops and portable electronic devices. On a periodic basis, at least annually, revisit security awareness to demonstrate the consequences of desktop, laptop and portable devices theft.**
- **Perform yearly HIPAA & HITECH security assessments. Protected health information, whether electronic or paper, is always vulnerable to a breach. An information security risk assessment will identify any gaps or inadequacies in your policies and procedures, and will provide recommendations to protect your sensitive information.**

To prevent theft:

- **Create a new policy and procedure that specifically addresses verifying the identity of critical vendors such as disposal and IT.**
- **Encrypt new and existing laptops. If encryption is not feasible, CEs and BAs should evaluate the business need to keep protected health records on laptops or mobile devices.**
- **Retrain all employees on all information security policies and procedures.**
- **Evaluate procedures and identify areas of risk that can increase the risk of theft.**
- **Review policies and procedures for safeguarding the physical security of paper records.**
- **Perform yearly physical and logical penetration tests.**

To prevent loss:

- **Evaluate procedures and identify areas of risk that can increase the risk of loss. For example, a covered entity which experienced a loss may continue to backup data on tapes, but after the breach it has learned to store the tapes in a safe deposit box instead of sending them via mail.**
- **Transfer the risk by contracting qualified vendors to handle certain operations such as the mailing of invoices.**

To prevent other:

- **Retrain all employees on all information security and privacy policies and procedures.**
- **Perform detailed annual risk assessments.**

To prevent incorrect mailing:

- **Through periodic audits, verify that outsourced mailing service providers have controls to prevent and detect errors incorrect mailings and these are operating effectively.**

To prevent unauthorized access:

- **Retrain all employees on all information security and privacy policies and procedures.**
- **Review and evaluate password policies and disposal procedures for storage devices such as file cabinets and media.**
- **Perform yearly logical penetration tests.**

Research Methodology

This report was generated by analyzing the electronic health information breaches disclosed in the U.S. Department of Health & Human Services and Health Information Privacy, Breaches Affecting 500 or More Individuals Report. The data was compiled over a one year period ranging from September 24, 2009 to September 23, 2010. The data was cross referenced to identify trends and risks based on this historical data.

References

- **U.S. Department of Health & Human Services, HIPAA Administrative Simplification Statute and Rules http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html**
- **American Recovery and Reinvestment Act of 2009**
- **Health Breach Notification Rule; Final Rule (18 CFR Part 318)**
- **Health Insurance Reform: Security Standards; Final Rule (45 CFR Parts 160, 162, and 164)**
- **Breach Notification for Unsecured Protected Health Information; Interim Final Rule (45 CFR Parts 160 and 164)**
- **HITECH Act Breach Notification Risk Assessment Tool prepared by NCHICA Privacy and Security Officials Workgroup www.nchica.org/HIPAAResources/Samples/BreachTool.doc**

About Kaufman, Rossin & Co.

Kaufman, Rossin & Co. is one of the largest accounting and consulting firms in the southeastern United States, with proven expertise in audit, tax and advisory services. Kaufman, Rossin's technology, processes and team help healthcare organizations perform HIPAA privacy audits, data mapping and inventory, risk assessments, vendor due-diligence, penetration tests, vulnerability scans, security breach response, and digital forensics to help organizations comply with HIPAA and HITECH while minimizing costs and risks.

Contact info:

Jorge Rey, CISA, CISM, CGEIT
jrey@kaufmanrossin.com
(p) 305.646.6076

Tyler Quinn, CPA, CISA
tquinn@kaufmanrossin.com
(p) 305.646.6111