A Look Back: U.S. Healthcare Data Breach Trends

A retrospective analysis of U.S. healthcare data breaches affecting 500 or more individuals

Authors: Chris Hourihan and Bryan Cline, Ph.D. for Health Information Trust Alliance (HITRUST)

December 2012
# Table of Contents

Executive Perspective ........................................................................................................... 3
State of the Industry .................................................................................................................. 3
Physician Practices .................................................................................................................. 4
Business Associates ................................................................................................................ 5
Government Institutions ........................................................................................................ 6
Paper Records ........................................................................................................................ 6
The Un-Reported ..................................................................................................................... 7
Recommendations .................................................................................................................. 8
Findings and Analysis .............................................................................................................. 10
Overview of the Data .............................................................................................................. 10
The Numbers at a Glance ....................................................................................................... 12
History of Breaches ................................................................................................................ 14
Breaches by Organization Type ............................................................................................ 16
Breaches Implicating Business Associates .......................................................................... 18
Identification and Notification of Breaches ........................................................................ 20
Type and Source of Breaches ............................................................................................... 21
  Type .................................................................................................................................... 21
  Source ............................................................................................................................... 22
  Type and Source .............................................................................................................. 23
Types of Breaches by Organization Type ........................................................................... 26
Macro Analysis ........................................................................................................................ 28
  Physical Vs. Electronic ...................................................................................................... 29
  Insider Vs. Outsider Threat ............................................................................................... 30
  Accidental Vs. Malicious Intent ....................................................................................... 31
  Multiple Breaches .......................................................................................................... 32
Cybercrime ............................................................................................................................. 32
  Hacking ............................................................................................................................. 32
In Conclusion .......................................................................................................................... 37
Recommendations ................................................................................................................ 38
How HITRUST Is Adapting .................................................................................................. 43
Executive Perspective

It has been more than three years since the breach notification requirements of the Health Information Technology for Economic and Clinical Health (HITECH) Act went into effect. Since that time, the industry has witnessed a steady flow of breaches where the number affected was over 500 individuals. The number of breaches totaled 495 as of October 1, 2012. There has also been an alarmingly high number of breaches where the number of individuals affected was under 500 individuals, totaling over 57,000 as of May 2012\(^\text{ii}\). While the details of those breaches affecting less than 500 individuals are not published, the U.S. Department of Health and Human Services (HHS) continues to make available the details of those over 500 individuals\(^\text{ii}\). This data coupled with the information obtained through HITRUST CSF assessments provides the foundation for our analysis.

State of the Industry

How has the industry been fairing? The industry has improved slightly since breach reporting became mandatory in September 2009, but recent spikes make it unclear whether improvement will continue. At a macro level, the number of breaches experienced and posted quickly reached a peak, leveled off, and appears to be on a steady decline, as seen in Figure 1.

![Figure 1 – Total Number of Breaches in Healthcare per Quarter](image)

While the good news is that reportable breaches do not appear to be becoming any more pervasive, the bad news is that the industry’s progress appears to be slow. Looking at some of the specifics, the organizations, types of breaches, and the sources of the breached data remain fairly consistent year over year, or demonstrate an increase following an initial decline.
Of the consistently most breached organization types, only hospitals and health plans maintain forward momentum, demonstrating a decline year over year. The only category to not see any decline in 2011 and, based on what we have seen to-date and projected for the entirety of 2012, is physician practices.

<table>
<thead>
<tr>
<th>Breaches by Organization Type</th>
<th>2010</th>
<th>2011</th>
<th>2012 (Q1 and Q2)</th>
<th>2012 (Projected)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hospital/Health System</td>
<td>82</td>
<td>48</td>
<td>14</td>
<td>41</td>
</tr>
<tr>
<td>Physician Practice</td>
<td>48</td>
<td>48</td>
<td>24</td>
<td>54</td>
</tr>
<tr>
<td>Health Plan</td>
<td>25</td>
<td>22</td>
<td>6</td>
<td>19</td>
</tr>
<tr>
<td>Academic Medical Center</td>
<td>16</td>
<td>6</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>Government Agency</td>
<td>12</td>
<td>4</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>Academic Institution</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>11</td>
</tr>
</tbody>
</table>

For breaches where a Business Associate (BA) is explicitly listed, by the raw numbers we’re expecting a 6% decline for 2012. Looking at breaches implicating a BA as a percentage of total breaches, we’re expecting a 1.1 point decrease from the 2011 to 2012.

<table>
<thead>
<tr>
<th>Breaches Implicating a Business Associate</th>
<th>2010</th>
<th>2011</th>
<th>2012 (Q1 and Q2)</th>
<th>2012 (Projected)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BA Implicated (#)</td>
<td>44</td>
<td>34</td>
<td>15</td>
<td>32</td>
</tr>
<tr>
<td>BA Implicated (%)</td>
<td>20.9%</td>
<td>22.4%</td>
<td>22.7%</td>
<td>21.3%</td>
</tr>
</tbody>
</table>

Of the types of breaches most often experienced, theft continues to dominate as the most likely cause of a breach in healthcare. An interesting point to note is that based on the number of hacks reported for 2012, we are expecting a 50% in these types of breaches or 2012.

<table>
<thead>
<tr>
<th>Breaches by Type</th>
<th>2010</th>
<th>2011</th>
<th>2012 (Q1 and Q2)</th>
<th>2012 (Projected)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft</td>
<td>107</td>
<td>82</td>
<td>41</td>
<td>88</td>
</tr>
<tr>
<td>Loss</td>
<td>34</td>
<td>15</td>
<td>6</td>
<td>13</td>
</tr>
<tr>
<td>Unauthorized Access/Disclosure</td>
<td>22</td>
<td>20</td>
<td>5</td>
<td>17</td>
</tr>
<tr>
<td>Incorrect Mailing</td>
<td>10</td>
<td>10</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>Improper Disposal</td>
<td>11</td>
<td>9</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>Hack</td>
<td>11</td>
<td>8</td>
<td>6</td>
<td>12</td>
</tr>
</tbody>
</table>

The source of breached protected health information (PHI) across the board is in a state of flux, with four of the six categories listed experiencing a decline between 20% and 50%. However, what has always been a hot button issue for the industry is breaches involving laptops, of which we continue to see high numbers and expect totals close to 2010 this year.

**Physician Practices**

The biggest issue in this industry continues to be stolen devices, with laptops the clear target, and with independent physician practices and specialty clinics suffering from the biggest losses. Business associates continue to pose a significant
threat to the industry as a whole, and physician practices and specialty clinics in particular, with slightly more than 30% of all breaches of these types of organizations implicating a business associate.

Larger practices with greater resources appear to be recognizing the problematic threats resulting in breaches and many seem to be taking actions to prevent future breaches. For example, Hospitals and Health Systems experienced a 46% decline in breaches from 2010 to 2011, and we are expecting a 36% decline from 2011 to 2012. Stage 1 meaningful use may have incentivized and/or raised awareness for the need for security, particularly in the most likely areas. Although physicians are similarly motivated, they continue to demonstrate a lack of progress.

It’s interesting to note that the size of an organization and its propensity for suffering a breach appear to be different between physician practices and the industry as a whole. Figure 2 shows the largest source of breaches occurs in smaller practices whereas Figure 3 clearly indicates larger institutions more likely to suffer a breach.

![Figure 2 – Percentage of Breaches for Physician Practices by Size](image1)

![Figure 3 – Percentage of Breaches for Healthcare Industry by Size](image2)

However, this risk is not just isolated to the practices themselves. Physician practices are increasingly accessing the systems of larger institutions. The adoption of electronic health record (HER) technology among hospitals, for example, has led to “community health records” where physicians utilize a local hospital’s EHR system instead of purchasing their own. This now exposes the hospital to the same risks as the connecting practices, which often lack anti-malware, have insecure or no firewalls, and share passwords. These issues in turn may lead to more breaches implicating both parties in the future.

**Business Associates**

Business associates continue to suffer from a lack of attention, and again, Physician Practices appear to be the primary organizations that have not yet learned how to effectively address the issue.
This is evidenced by the marked increase in the number of breaches with Physician Practices that implicate a business associate this year. While notably more challenging to effectively manage for small organizations that lack relevant resources, it also continues to be a challenge for what are typically the largest organizations, which are health plans. Likely a function of the sheer number of business associates a health plan has, often in the hundreds if not thousands, effective third party management continues to plague this group of organizations.

Government Institutions
While private industry and the generally smaller organizations are challenged, it is interesting to note that federal and state government institutions (including Veterans Affairs hospitals and medical centers) have similar issues with keeping patient records private, and account for 40% of all records breached since 2009. While many of these are attributable to a few high profile breaches such as TRICARE in September 2011, for the past two years government institutions have exceeded two million records breached, with 1.02 million already for 2012. The types of breaches occurring at these institutions are largely the same as those in other segments—lost and stolen laptops, desktops, mobile media and paper records. Government organizations have been the largest target of hacks by record count alone (close to 1.3 million records breached in this way), but again this is limited to a few high profile instances as opposed to it being a pervasive problem. What is clear is that government agencies are not setting a high bar for the rest of the healthcare industry.

Paper Records
Sometimes we forget in this age of electronic information that paper records still exist, still have sensitive data on them, and can be just as easily lost, stolen or otherwise breached. Since 2009, paper records have comprised 24% of healthcare breaches, second only to laptops; however, in a count of records, they remain a low 4%. Nonetheless, a breach is still a breach and paper record breaches also require notification. As seen in Figure 4, theft, improper disposal and unauthorized access are among the largest types of paper-based breaches. Also significant and rather unique to the physical medium, incorrect mailings are a leading cause of paper breaches.
We are seeing some improvement. On average, the industry has seen these types of breaches reduced by about 16% from 2010 to 2011. This may be attributable to the conversion from paper to electronic health records, but in light of this a word of caution is merited. While the impact may be small and things may be getting better, organizations making the transition from paper to electronic records should not lose sight of the need for continuous security throughout the process. As records are scanned or otherwise copied into EHR and other systems, it is easy for them to be misplaced since they may not be in their normal, secure location. In too many instances, boxes and binders of records are left unattended and disappear. Employees take records home that are subsequently stolen or go missing, and information is discarded in trash cans and recycling bins without first being shredded.

**The Un-Reported**

What is surprising from this data is the relative insignificance of the number of breaches being reported, less than 0.07%, compared with an estimated 700,000 covered entities and countless more business associates that maintain or access PHI according to the Breach Notification Interim Final Rule. HITRUST’s assessment data suggests that the security postures of organizations generally do not vary drastically, which would suggest that many breaches may go un-reported or un-discovered. The “Second Annual Benchmark Study on Patient Privacy and Data Security” by the Ponemon Institute supports this assertion, as 57% of healthcare organizations responding to the survey had little to no confidence in their ability to detect all data loss or theft.

One area we believe breaches are occurring, but are not accurately reported, relate to cyber threats including losses from malware and hacking. While collectively hacking and malware breaches only comprise 8% of the total breaches and 11% of the records breached, we have identified numerous instances of healthcare data on underground message boards that cannot be tied back to a reported breach. Below are a few examples referenced in recent HITRUST Cyber Threat Intelligence reports published by the HITRUST Cyber Threat Intelligence and Incident Coordination Center:


![Image of a PHI database]

- Russian-speaking actor "pronto" offered to sell an online pharmacy database containing 45,000 records.

- English-speaking actor "Bresti" advertised a database containing 17,000 health insurance records of California residents.

- English-speaking actor “bau1” recently advertised a database on a prominent cybercrime forum containing personally identifiable information (PII) and PHI, including names, addresses, Social Security numbers, dates of birth and some health history details. Bau1 specified a price of $2.00 USD per individual record with a minimum order of 500 records per transaction, but he did not specify how many entries the purported database contained.
Unfortunately we cannot confirm that any of these breaches were reported by the affected entities because we do not know who they are; cross-referencing the totals, even accounting for a margin of error, reveals no obvious targets.

Further, we receive frequent inquiries and feedback from IT, security and audit professionals in healthcare who know their EHR and other clinical technologies are vulnerable but cannot implement adequate protection because the vendors are unwilling to disclose or communicate these risks.

The reasons behind this disconnect between what the HHS breach data conveys and the input we receive from other sources is not entirely clear, and it is likely the causes are many. For example, it is possible the breaches associated with these insecurities do not involve PHI and instead focus on demographic, proprietary and/or financial information. It is also possible that some breaches, though not the ones cited above, individually involved fewer than 500 records. Or it could be that healthcare organizations simply lack the ability to consistently identify these types of breaches. Lost and stolen devices on the other hand are fairly simple to detect and may be diverting an inordinate amount of time and resources from other cyber threats.

Regardless, it is apparent that the true nature of cyber threats is not clearly understood by the healthcare industry. If we can learn anything from other industries with more experience dealing with cyber threats, it is that healthcare—especially larger entities with more data and more third party connections—should be seriously mindful of cyber threats and increase their efforts to protect against them.

**Recommendations**

The data continues to send a clear message that endpoint and mobile media security are areas that require serious attention, organizations need to continue to maintain rigid processes in converting from paper to electronic systems, organizations must conduct the necessary due diligence for business associates, and we must find a way to reach physician practices and provide them with simple cost-effective solutions to their biggest security challenges.

- **Endpoint Security**
  - Conduct an accurate inventory of endpoint devices and develop a “bring your own device” (BYOD) policy and management program.
  - Ensure email access is controlled and encrypt email
  - Encrypt mobile computing devices and consider encrypting desktops
  - Ensure less mobile endpoints such as servers are adequately protected

- **Mobile Media Security**
  - Restrict the use of unencrypted mobile media, including backup media such as unencrypted tapes

- **Paper Records**
  - Ensure paper records are adequately secured when transitioning to an EHR system
  - Make employees aware of proper handling and disposal procedures
  - Provide an adequate number of shredders or shredding bins in convenient locations
• Ensure bins are emptied regularly and require onsite shredding if possible
  • Centrally store and manage paper records in a secure location

* Business Associates (BA)
  • Formally assess and manage the risks incurred with a BA
  • Classify and manage risks based on impact and likelihood of a breach by the BA
  • Periodically re-evaluate BAs based on changing risks but no less than every three years
  • Limit BA access to only the information minimally necessary to conduct business

* Physician Practices
  • Treat physician practices that connect to your organization as high risk
  • Require similar assurances from physician practices that you obtain from BAs
  • Ensure risks are comprehensively assessed: administrative, technical and physical
  • Minimize effort by leveraging existing resources from HHS, HITRUST and others

A more comprehensive discussion of these recommendations may be found at later in this report.

Note, these recommendations should not be construed as a plan for a comprehensive security program; instead, they provide strong starting points for security initiatives based on lessons learned from three years of healthcare breach data.
Findings and Analysis

Overview of the Data

Breach reporting and posting to the HHS website began in September 2009. With each incident, the following information is provided:

- Name of the covered entity
- Name of the business associate(s) involved, if any
- State in which the breach occurred
- Number of individuals affected
- Date of breach
- Type of breach
- Source of breach
- Date posted/updated
- Summary of what occurred, if any

We supplemented the HHS data (e.g., by adding organizational size) and categorized the new data set as noted below:

- **Type of Organization**
  - Academic Institution – Universities and other institutions that offer education as the primary service. The field of education may be, but is not required to be, specialized to healthcare, such as schools of medicine.
  - Academic Medical Center – Hospitals affiliated with a university or other academic institution.
  - Durable Medical Equipment Providers – Vendor organizations that provide and sell medical devices, medical supplies, and other equipment to aid in the delivery of care.
  - Financial Services – Organizations, banks, and funds that primarily manage money (e.g., Flexible Spending Account (FSA) fund managers).
  - Government Agency – Federal, state, and local agencies excluding military and Veterans Affairs (VA) hospitals, medical centers or health systems.
  - Health Plan – Carriers of health insurance including Medicaid/Medicare carriers, state plans, and veteran’s coverage.
  - Home/Hospice/Extended Care Facility – Facilities providing long-term care, in-home care or care management for the elderly, terminally ill, or seriously ill.
  - Hospital/Health System – Hospitals, medical centers and systems of providers, including specialties, that offer inpatient care services including military and VA medical centers, hospitals, and health systems.
  - Insurance (General) – Carriers of insurance other than health insurance (e.g., life).
  - Lab – Medical testing centers.
  - Other Ambulatory Care – Ambulance, emergency services, and rescue.
Outpatient Care – Organizations offering social, family and community outreach programs including limited or short-term care.
- Pharmacy/Pharmaceutical – Retail pharmacy or drug manufacturers.
- Physician Practice – Offices of MDs (e.g., doctor offices, dentists, specialty practitioners).

- Government – Determination if the organization is directly or closely affiliated with the provision of federal, state, local or military services, including all agencies, state, military, Medicare/Medicaid insurance plans, and VA providers.

- Size (by employees)
  - 1 – 10
  - 11 – 100
  - 101 – 1,000
  - 1,001 – 10,000
  - 10,000+

- Date Discovered – If available via the official notification released for the breach, news coverage, Privacy Rights Clearinghouse, PHIprivacy.net, and/or DataLossDB.org.

- Time to Discovery – Count of the days between the date the breach occurred and the date the breach was discovered by the organization, if available.

- Time to Notify – Count of the days between the date the breach was discovered and the date the breach was posted/updated, if available.

- Type of Breach (Modified) – Adjusted set of breach types
  - Error/Omission – Errors or omissions in the configuration of devices (e.g., servers) or applications.
  - Hack – Deliberate cyber-attacks by an outsider on an organization’s network, systems, or applications.
  - Improper Disposal – Disposal of information (paper or electronic) that is not in accordance with the guidance published in the Breach Notification Rule to render PHI unreadable, unusable, or indiscernible.
  - Incorrect Mailing – Physical mail that is sent to the incorrect individual, allows unauthorized access to PHI during the normal course of mailing (e.g., PHI visible through envelope windows), or provides more information than would normally be allowed in the course of business to a third party.
  - Loss – Endpoint devices, media, or physical records that are lost or misplaced.
  - Malware – Infections of malicious code on organizations network and/or devices that typically results in the exfiltration/compromise of sensitive data.
  - Theft – Endpoint devices, media, or physical records that are deliberately taken from the organization responsible for maintaining the device, media, or records.
  - Unauthorized Access/ Disclosure – Physical or electronic records that are accessed by an unauthorized individual (insider or outsider) but the records were not permanently removed from control by the organization responsible (Note: any electronic breaches involving an outsider that are deliberate attacks against the organization’s network or
systems, even if the attacks are not deliberately after PHI, would not be classified as Unauthorized Access/Disclosure and would instead be classified as a Hack).
  o Unknown – Breaches where the nature of the cause of the breach is not known or disclosed.
  
  • Source of Breach (Modified) – Adjusted set of breach sources (referred to as “location” by HHS).
    o Desktop Computer – Computer devices where the unit containing the CPU is separate from the monitor and other I/O devices.
    o Email – Electronic mail and any attachments to electronic mail.
    o Laptop – Computer devices that are self-contained but with a clam-shell form factor (distinguishing laptops from tablet computing devices).
    o Medical Device – An instrument, apparatus, implant, in vitro reagent, or similar or related article that is used to diagnose, prevent, or treat disease or other conditions, and does not achieve its purposes through chemical action within or on the body.
    o Mobile Media – Includes USB flash drives, external hard drives, backup tapes, CDs/DVDs, or other forms of electronic storage that provide limited if any functionality beyond storage.
    o Multiple – Breaches involving one or more sources.
    o Network Server – Computer devices that serve the needs of other computers on a network.
    o Paper Records – Physical pieces of paper or groups of paper.
    o Phone/Tablet – Mobile computing devices that run mobile operating systems, may be primarily operated by touch, and/or provide cellular telephony.
    o System/Application – Computer code that performs a certain function or set of functions and runs on an endpoint computer device.
    o Unknown – Breaches where the source of the PHI breached is unknown or unreported.
    o X-ray Films – Photographic film used to make X-ray pictures.
  
  • Physical/Electronic – Was the source of the breached data in physical or electronic form.
  • Insider/Outsider – Was the breach caused by an employee of the covered entity or an outsider (Note: business associates are not classified as either and are reported as a separate category since business associates are neither true outsiders nor insiders).
  • Accidental/Intent – Was the breach the result of an accident or a deliberate act to breach PHI
  • Breach History – List of any prior breaches the organization has experienced, including those unrelated to PHI

The Numbers at a Glance

<table>
<thead>
<tr>
<th>Total breaches:</th>
<th>495</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total records:</td>
<td>21.12M</td>
</tr>
<tr>
<td>Total cost:</td>
<td>$4.1B</td>
</tr>
<tr>
<td>Average size:</td>
<td>42,659.1 records</td>
</tr>
<tr>
<td>Average cost:</td>
<td>$8.27M</td>
</tr>
<tr>
<td>In 2012 (as of 1 Oct):</td>
<td>77</td>
</tr>
<tr>
<td>In 2011:</td>
<td>152</td>
</tr>
<tr>
<td>In 2010:</td>
<td>210</td>
</tr>
<tr>
<td>Largest breach:</td>
<td>TRICARE Management Activity, Sept-2011, 4.9M records</td>
</tr>
<tr>
<td>Most breached organizations:</td>
<td>Hospitals/Health Systems and Physician Practices were responsible for 32% and 28% of the total breaches, respectively.</td>
</tr>
<tr>
<td></td>
<td>Government Institutions (which includes VA hospitals) have experienced the greatest loss of records, with 40% attributable.</td>
</tr>
<tr>
<td></td>
<td>Since July 2011, Physician Practices have become the most breached organization type, surpassing Hospitals/Health Systems.</td>
</tr>
<tr>
<td></td>
<td>Health Plans have not posted any breaches since Q1 2012.</td>
</tr>
<tr>
<td></td>
<td>California, Texas, and New York respectively have the highest number of breaches.</td>
</tr>
<tr>
<td></td>
<td>Per Capita, Washington DC, Alaska, and Puerto Rico experienced the most breaches.</td>
</tr>
<tr>
<td></td>
<td>BAs are implicated in 21% of the breaches.</td>
</tr>
<tr>
<td></td>
<td>BAs have accounted for 58% of the records breached.</td>
</tr>
<tr>
<td>Average time to identify:</td>
<td>84.78 days</td>
</tr>
<tr>
<td>Average time to notify:</td>
<td>68.31 days</td>
</tr>
<tr>
<td></td>
<td>50% of all organizations are falling behind the 60 notification deadline set by HITECH.</td>
</tr>
<tr>
<td>Leading cause:</td>
<td>Theft (54%)</td>
</tr>
<tr>
<td>Leading sources of breached PHI:</td>
<td>Laptops (25%) and Paper Records (24%)</td>
</tr>
<tr>
<td>Most stolen items:</td>
<td>Laptops, Desktops, and Mobile Media (USB drives, CDs/DVDs, backup tapes)</td>
</tr>
<tr>
<td></td>
<td>Theft and Loss</td>
</tr>
<tr>
<td>Most likely cause of breached electronic records:</td>
<td>Theft, Incorrect Mailing and Improper Disposal</td>
</tr>
<tr>
<td>Most likely cause of breached paper records:</td>
<td>70% of breaches involved electronic data and accounted for 96% of the records breached.</td>
</tr>
<tr>
<td>Physical vs. Electronic¹:</td>
<td>26% of breaches involved physical data but</td>
</tr>
</tbody>
</table>

¹ The location and storage medium (electronic versus physical) was not known for 3% of the breaches reported.
History of Breaches

Following the breach notification requirements, the industry saw a sharp, three-quarter increase in the number of breaches reported, as shown in Figure 5. For a full year following the second quarter of 2010, there was a slight but steady decline in the number of breaches experienced and reported by healthcare organizations. This was maintained for yet another year through the second quarter of 2012, with quarterly peaks and valleys. Looking at the trend line, it is clear that at this point the number of breaches has decreased from a high of 57 in the second quarter of 2010 to a low of 24 in the second quarter of 2012, or about 58%.

Figure 5 – Total Number of Breaches in Healthcare per Quarter
Looking at the sum of the total records breached by month in Figure 6 reveals an increasing trend line (based on a four period moving average) up until the third quarter of 2011, which has since been on a slight decline. A review of the median number of records breached per quarter in Figure 7, which addresses the issue of outliers, demonstrates an overall slight decline in the number of breached records quarter by quarter.

**Figure 6 – Total Number of Breached Records per Quarter**

**Figure 7 – Median Number of Breached Records per Quarter**
Breaches by Organization Type

By count alone, hospitals and physician practices are the most at fault, accounting for 32% and 28% of the total breaches respectively, as shown in Figure 8. Health plans are in a distant third, with 14%.

Breaking each segment down by the size of the organization, health plans, hospitals, government agencies, and academic medical centers—the leading segments for breaches—are largely 100 employees or greater (73%, 77%, 64%, and 65% respectively). On the other hand, 61% of Physician Practices breached were 100 employees or fewer.

Based on an SK&A survey conducted in January 2012\textsuperscript{x}, approximately 90% of practices have less than five physicians and 96% have less than nine. We can then assume that between 90% and 96% of all practices have 10 or fewer employees, which according to the HHS data accounts for 39% of all breaches for Physician Practices as a whole. Given that 17% of breaches at physician practices are of an unknown size, that number could be as high as 56%. Conversely, this would imply that between 4% and 10% of all practices account for between 44% and 61% of all breaches in this category.

Since a January 2012 SK&A survey on EHR adoption rates are significantly higher for larger practices than their smaller counterparts (30.8% for one-doctor practices as opposed to 75.5% for practices with more than 25 physicians), we determined that practices with less than 10 employees—between 90% and 96% of all practices—account for between roughly 82.4% and 92.5% of all EHRs and between 39% and 56% of all breaches. Conversely, practices with more than 10 employees—between 4% and 10% of all practices—account for about 8.5% to 17.6% of all EHRs and between 44% and 61% of all breaches. This would indicate that, of those with an EHR, larger practices (over 10 employees) are about four times more likely to suffer a breach of more than 500 records than smaller practices.

Unfortunately, we do not have access to HHS data for smaller breaches and cannot assess whether or not smaller practices are better or worse at protecting patient data overall. But the data does suggest...
this industry segment is struggling and requires significant assistance due to a lack of available expertise and resources.

Looking at the total records breached by each organization type in Figure 9, we find a much different picture.

By a far margin, health plans are responsible for the greatest loss of records, 10.32 million (49%), stemming from only 14% of the breaches reported. Although it demonstrates a significant decline in the total percentage of records breached, this is in line with our original May 2010, analysis that found health plans accounted for a vast majority of records breached (80%) although they only accounted for a relative minority of breaches (16%). This is understandable given the few but high profile breaches of plans since 2009. For instance, a single breach the TRICARE Management Activity experienced in late 2011 totaled 4.9 million records.

Yet organizations like TRICARE can also be classified as a government institution along with State Departments of Health, VA hospitals and county agencies. Looking more closely as the distribution of breaches by government versus non-government institutions, we find that while 10% of breaches are affiliated with the government in some way, this accounts for 40% of the records breached (see Figures 10 and 11).
Looking at these kinds of organizations more closely in Figures 12 and 13 reveals somewhat of a mixed bag. While federal, state and local government agencies are responsible for the largest percentage of breaches, the health plans (Medicare/Medicaid, state insurance, and coverage for Service Members and Veterans) are responsible for the most records breached.

While the breakdown of government institutions mirrors the overall industry results, the high number of breaches by agencies themselves compared with other categories is surprising. It is likely one of the reasons we see more breaches with other types of organizations than government agencies is because there are simply more of them. But within the government segment itself, agencies clearly present a higher risk in terms of number of breaches compared with providers and payers in the same category.

**Breaches Implicating Business Associates**

Business associates have always been a thorn in the side of healthcare organizations when it comes to breaches, responsible for between 20% and 30% of all breaches since 2009 as shown in Figure 14.
With few notable exceptions to this trend and without major changes to how healthcare entities approach business associates, we expect this to continue into the foreseeable future.

From a pure numbers perspective, business associates have accounted for 21% of the breaches experienced to date as shown in Figure 15. Yet, when we compare this with the number of records breached that implicate a business associate, we see a much different story, as shown in Figure 16.

This appears to be a high risk case where the impact, as opposed to likelihood, is the driving factor. It is understandable that when an organization engages a business associate, it is for a service that likely requires some level of access to PHI. Where we believe many organizations falter is not identifying and restricting access to what is actually required at a data, application, and network level. This leads to information leakage and ultimately high profile breaches when they do occur. It is also worth noting that this issue appears to be worsening from the perspective of record count. Our original analysis in May
2010 found that 17% of breaches and 7% of records breached implicated a business associate. We now see that 21% of the breaches implicating a business associate account for 58% of the records breached.

The problems business associates struggle with are largely the same as the rest of the industry. If we look at a breakdown in Figure 17 of the breaches implicating a business associate by breach type, we see the pervasive issue is again lost and stolen devices.

Abuse and misuse of access account for a significant 14% of breaches, which most frequently involves paper records. Incorrect mailing, e.g., where information is visible through the envelope window, letters are double stuffed, or individuals are associated with an incorrect address, is also significant, accounting for 12%.

Identification and Notification of Breaches

Overwhelmingly, most breaches were identified by organizations within 30 days of occurrence, as shown in Figure 18. Given that a majority of the breaches involved lost or stolen devices, this is not surprising. Across all breaches, the average time to identify a breach is 84.78 days, which is distorted by 11 breaches that took one or more years to identify.

For example, in the case of Riverside Mercy Hospital, patient and employee records were left in the hospital after the facility was sold to Toledo Public schools in 2003. Records were left unsecured in that facility from 2003 until they were discovered in November of 2010.

Removing outliers significantly reduces the industry’s average time to identify a breach to 20.77 days, which is less than but closer to the median of 39 days. What is surprising is that a majority of the hacking and malware outbreak incidents took less than 30 days to identify. The most difficult issue to identify quickly—or rather the one that is most likely to slip through the cracks—is unauthorized access/disclosures. A majority (55%) of these breaches went undiscovered for over 100 days, and slightly more (55%) were perpetrated by internal employees. While unauthorized access may only account for 11% of the breaches, the time it takes to identify such
breaches of this nature highlight the need for increased internal auditing and monitoring of employee access.

Since there are no regulatory requirements on the speed with which organizations must detect breaches, the interesting metric is the time it takes organizations to notify individuals, the secretary and the media following a breach of 500 or more individuals, as shown in Figure 19. In this situation, the industry is falling slightly behind, with an average time to notify of 68.31 days and a total of 50% of organizations out of compliance with the 60 day notification deadline.

The reason for this is unclear based on the data alone. Looking at the types of organizations, types of breaches and business associate involvement as a percentage of the total breaches within each category, there are no clear trends. What is noticeable is that organizations in general have been getting worse for the past three quarters. As shown in Figure 20, with the exception of a one-year period between the Q4 of 2010 and Q3 of 2011, a majority of breaches as a percentage of total breaches have taken 61 or more days to report.

**Type and Source of Breaches**

**Type**

How are breaches occurring? Largely, little has changed in the past three years. As Figures 21 and 22 depict, theft is overwhelmingly the leading cause of breaches, accounting for 54% of the total breaches.
and 37% of the total records breached. Loss is the second leading cause, accounting for 12% of breaches and 45% of the total records.

Turning attention to the timeline in Figure 23, it is clear to see that theft has been the leading problem since 2009.

Theft, loss and unauthorized access have remained dominant, even if only slightly, for the past three years. Further, the plot of theft mirrors that of the total breaches with the round arc from September 2009 through January 2011 and the two spikes in Q3 and Q1 of 2011 and 2012, respectively. This is not surprising given that theft is by far the largest category of breaches.

**Source**

A review of breach types cannot be effectively done without a review of breach sources, as shown in Figures 24 and 25. Presenting a slightly more evenly distributed picture than breach types, breaches
have primarily occurred due to PHI on laptops, paper, mobile media and desktop computers. Yet looking at the distribution by count of records breached, mobile media accounts for 51%, followed by network servers (17%), and laptops (12%).

The timeline in Figure 26 tells a similar story, with breached laptops, paper records, and mobile media as the leading sources of breached PHI.

**Type and Source**

Reviewing the type and source together in Figure 27, the theft of laptops is the leading cause of breaches, accounting for 23% of all healthcare data breaches. Comparing this figure with the one from our original analysis of the data back in May 2010, we find they are essentially the same (there were 16 instances of theft of laptop out of a total of 69 reported breaches, or 23.18%).
The most notable difference is that desktops are now stolen more than mobile media, even if only slightly, which helps make a case for the expanded scope of encryption to include all endpoints, particularly those in public or easily accessible sources. This is in line with the direction Stage 2 meaningful use is headed, which requires eligible hospitals and physician practices to implement encryption of data at rest or document a risk analysis as to why the data is not encrypted. Of course this issue is one that can and should be applied more broadly to all organizations in healthcare. The silver lining may be that these devices are likely stolen for their value alone and not because of the data.

![Figure 27 – Total Number of Breaches by Location and Type](image-url)
We find a noticeable change when switching from a count of the breaches to the sum of the records breached as shown in Figure 28. Lost mobile media accounts for 36% of the records breached, with stolen mobile media adding another 15.5%.

This is not surprising because the problems experienced over the last two years are largely unchanged. The difference between theft and loss is almost moot and both could be combined into a single category because they may be mitigated by the same control: encryption. While HITRUST’s focus has expanded...
from laptops and mobile media to all endpoints (including network servers) given the increasing numbers in these categories, the underlying issues are not changing. The industry is still struggling with the fundamentals and, for at least the near term, will likely continue to do so.

Types of Breaches by Organization Type
Which organizations are at risk for what types of breaches? Quite simply, hospitals and physician practices are the most likely to be victims of theft, as shown in Figure 29. Although physical access controls to sensitive areas in patient care facilities are arguably on par with many of their counterparts in the industry, the simple fact is hospitals, health systems and physician practices routinely see significantly more visitors—patients and their families in particular—than health plans, insurance companies and vendors.
While not nearly as prominent, unauthorized access and disclosures among the major types of healthcare institutions (health plans, hospitals and government agencies) consistently shows up as a leading cause of breaches. Given the difficulty in controlling access in environments where many employees require, or demand, ubiquitous access, it is understandable why this is and continues to be a problematic area. But what are we not seeing? Why is it not more prominent?

We suspect that this category of breach is more significant than the data reveals, but is not as readily reported. First, many organizations simply have a hard time detecting these types of breaches, particularly on a smaller scale. To detect unauthorized accesses like snooping in an electronic environment, organizations require sophisticated monitoring software that can analyze each access and correlate it with other factors such as frequency of access for the individual, department, and time of day to name a few. Second, we believe an overwhelming majority of these breaches are under 500 individuals and therefore reside among the other 57,000-plus breaches on which HHS has collected data since late 2009. Since we do not have access to this data, we can only hypothesize, but the assertion is consistent with HITRUST’s experience working with healthcare organizations.

We can see in Figure 30 that hospitals and health systems have been getting noticeably better at controlling the loss and theft of devices.

![Figure 30 - Total Number of Losses and Thefts for Hospitals/Health Systems per Quarter](image)

It is likely we are seeing this trend due to the requirements of meaningful use. Since HITECH, meaningful use has been the most prominent regulatory requirement to impact this segment. But it also applies to physician practices, and while we would expect a similar trend, it is clearly a different story.
Looking only at theft as shown in Figure 31—loss is actually a low cause for this group—our trend line is essentially flat from 2009 through today. Why is there a difference if both physicians and hospitals are subject to meaningful use? Well, we may be able to account for this by looking at the rate of adoption and attestation for meaningful use. In reviewing the data Centers for Medicare & Medicaid Services (CMS) makes available along with other sources\(^\text{x}\) regarding attestation and payment compared with the counts of hospitals and physicians from the American Hospital Association\(^\text{xi}\) and American Medical Association\(^\text{xii}\), we estimate that only about 22% of office-based physicians have adopted an EHR and received payment compared to approximately 55% of hospitals and health systems. If one considers that only an estimated 46% to 47.5% of all practices have an EHR\(^\text{xiii}\) (an increase of 6% since Jan 2011), this means that roughly half of those practices have successfully attested to meaningful use. In contrast, between 63% to 73% of hospitals and health systems have an EHR\(^\text{xiv}\), which means a significantly higher percentage of hospitals that have adopted an EHR have satisfied meaningful use requirements (between 75% and 87%) compared with practices (between 46% and 48%). While not definitive, this may very well explain the improvement we’ve seen in hospitals compared to physician practices.

**Macro Analysis**

Something new we have done with this analysis is a review of macro-level elements based on, but not directly reported in, the data. Much of this requires further research and analysis into the nature of the breach, relying heavily on the actual notices of the organizations breached and the explanation of the breach contained therein. Unfortunately, this leads to an imperfect set of data where, for example, we are unable to determine with certainty if a breach was intentional or not. Yet, it still provides value in understanding if and how things are changing.
Physical Vs. Electronic

By far, the most breaches and the greatest loss of records are associated with electronic information as shown in Figures 32 and 33.

![Figure 32 – Percentage of Breaches by Electronic/Physical](image)

![Figure 33 – Percentage of Breached Records by Electronic/Physical](image)

Both findings are understandable. Electronic information is more easily breached in large quantities given its ease of transport, export or copying. Physical breaches of PHI are fairly evenly distributed between theft, incorrect mailing, improper disposal, and unauthorized access, but almost 90% involved less than 10,000 records of individuals (compared with 75% for breaches of electronic information). Of the largest breaches of paper records, 36% were due to incorrect mailing of records and 29% were due to improper disposal of records.

A view of the timeline in Figure 34 reveals, with the exception of Q1 in 2011 and Q4 in 2012, a fairly flat trend of about 30% of all breaches involving paper records since September 2009.

![Figure 34 – Percentage of Breaches by Electronic/Physical per Quarter](image)
Yet, a review of recent periods from 2011 to present suggests that while the number of electronic breaches remain flat, physical breaches are trending significantly downward, as shown in Figure 35. It is highly possible the conversion of paper records to electronic form, and subsequently the decreased amount of paper records that organizations maintain, is leading to this trend.

![Figure 35 – Total Number of Electronic/Physical Breaches from 1/1/2011 to 6/30/2012](image)

**Insider Vs. Outsider Threat**

The insider versus the outsider threat is a hotly debated issue in the field of security and one that has been waged for some time. While each industry is different, in healthcare outsiders are the leading cause of breaches, and third parties, depending on how you classify them, are the leading cause of breached records, as shown in Figures 36 and 37.

![Figure 36 – Percentage of Breaches by Insider/Outsider/Third Party](image)

![Figure 37 – Percentage of Breached Records by Insider/Outsider/Third Party](image)
If one considers the broader interpretation of insider as someone that has authorized access to corporate data, then the inclusion of business associates raises the numbers for insider threat to 44% of breaches and 71% of records breached.

It is worth mentioning that this data may not be telling a completely accurate picture. Outsiders include thieves whose intent is unknown but may be focused on the device versus the data. Further, this analysis only considers breaches affecting 500 or more individuals. If we had HHS’s complete data set of over 57,000 breaches, one can speculate that, while little may change with the percentage of total records breached, it would be different with the number of breaches. It is possible that many insider breaches are the occasional snooping at one or two records or practitioners accidentally or intentionally taking select patient records home but not in mass quantities. While these cases may not result in significant penalties and negative press, HITRUST’s experience suggests that organizations remain mindful of the insider threat through strong access, authorization and monitoring controls.

**Accidental Vs. Malicious Intent**

Although intent is one of the most difficult macro-level views to analyze due to a general lack of information (as seen from the large percentage of unknown causes in Figures 38 and 39), we found that at least 11% of the total breaches and 13% of the total records breached were intentional. Given the high number of reported breaches due to loss (12% accounting for 45% of records breached), it is not surprising to find that 26% of the total breaches and 50% of all of the records breached were accidental. In addition to loss, incorrect mailings and application errors that accidentally exposed records were commonly reported causes.

![Figure 38 – Percentage of Breaches by Accidental/Intentional](image)

![Figure 39 – Percentage of Breached Records by Accidental/Intentional](image)

Unfortunately, the majority of breaches reported are a result of theft of devices where intent is unknown, giving us limited insight into the nature of cybercrime of healthcare data (see Cybercrime section below for further analysis).
Multiple Breaches

Finally, we looked at each organization that experienced a breach to determine if the organization had a history of breaches, whether of healthcare data or another sensitive type (e.g., financial or other personal information) sourced from datalossdb.org. We found that a quarter of all organizations had at least one prior breach that was reported, as shown in Figure 40.

While we expect a vast majority of organizations to have had at least one breach in the past, even if only relatively small, what is concerning is the rampant occurrence of large breaches at organizations that deal with healthcare data. The Office for Civil Rights (OCR) and HHS should pay special attention to organizations with multiple breaches to demonstrate that HIPAA truly does now have “teeth.”

Cybercrime

Cyber threats such as cyber terrorism, organized crime and hacktivism remain a major concern to large healthcare organizations and the industry as a whole. Given how cyber threat actors have attacked other industries, such as banking and retail and the increased availability of electronic PHI thanks to the adoption of EHR systems, we believe the healthcare industry is at high risk.

As previously discussed, known intentional breaches of PHI (11%) are in the minority and have largely remained constant. Analyzing the breakdown of these types of breaches (see Figure 41) reveals hacking and unauthorized access as the leading types of threats. It is worth noting that not all hacks and malware outbreaks are listed in this data set. Two instances of hacking were unknown in their intent due to lack of data, and a majority of malware outbreaks (89%) were unknown for a similar reason.

Hacking

Let us begin by reviewing the profiles of some of the intentional breaches caused by hacking:

- On June 25, 2012, The Surgeons of Lake County determined that an unauthorized user had gained remote access to one of the company’s servers, encrypting the server and the data of...
7,067 individuals. The malicious user demanded payment in return for the password to decrypt the server, posting a ransom note on the server. Upon discovery, the server was shut down by the organization and the police were notified.

- On March 10, 2012, computer hackers gained access to a Utah Department of Technology Services (DTS) computer server that stores Medicaid and Children’s Medicaid claims data. The hackers began removing personal information from the server on March 30, but it wasn’t until April 2 that DTS detected the breach and immediately shut down the server. By that time the hackers had stolen 280,000 Social Security numbers, as well as less-sensitive personal information of another 500,000 people.

- On February 23, 2012, a hacker gained access to one of the computers at a University of Houston (UH) College of Optometry neighborhood clinic and deleted the records of 7,000 individuals.

- On or about May 10, 2012, Choices, Inc. learned that its website and computer system was breached by an unknown, external hacker. Choices’ computer system stored a database file that contained health records created or received in the delivery of services to Choices’ clients. The data breached included individual social security numbers, demographic information and health information. It was later confirmed through forensic investigation that the information had been copied by the hacker.

- On December 5, 2011, Metro Community Provider Network became aware of a hacker potentially accessing the personal health information of some of its patients. In the incident a hacker sent an email to several of Metro Community Provider Network’s employees that claimed to be from a trusted source. The email asked for the employee to click on a link and provide login information. This was then used to gain access to the employee’s confidential emails containing PHI.

- Around May 9 - 10, 2011, multiple external intruders successfully gained unauthorized access to AssureCare Risk Management (ARM) systems. It appears likely that the unauthorized access originated from parties in China, Bulgaria and Texas. Forensic analysis determined that data stored by ARM on the hacked server included unencrypted personal health information, though it could not be confirmed nor denied that the information was copied.

- On September 21, 2010, Triple-S Salud learned from a competitor that a specific internet database managed by subsidiary Triple-C and containing information pertaining to individuals previously insured by Triple-S Salud had been accessed without authorization by the competitor’s employees from September 9 - 15, 2010. The forensic investigation revealed that the security breaches were the result of unauthorized use of one or more active user IDs and passwords specific to the database.

This is but a sample of the complete set of incidents; however, a review of all of the hacking incidents reveals the following:

- 11% were phishing attacks, though none of the attacks were targeted to specific individuals (e.g., executive management), resulting in employees exposing their email credentials.
11% were focused on destroying data or rendering it unusable to the organization in an attempt to blackmail the organization to regain access to the data.

7% were likely inadvertent whereby the hackers broke into the server to turn it into a gaming server.

15% of the attacks were related to corporate espionage.

The remaining 56% were various forms of unauthorized access by a hacker or group of hackers to one or more servers containing PHI, most likely for the purpose of copying and selling the data.

As defined in the recent HITRUST Cyber Threat Analysis Service (CTAS)™ “Cyber Threats to the United States Healthcare Sector” whitepaper, there are three primary actors in the cyber security sphere: cybercrime actors, espionage actors, and hacktivists. Based on the HHS breach data, 78% of the hacks can be attributed to cybercrime actors, 15% to espionage actors, and 7% as outliers.

Hacktivists were notably absent from the hacking incidents reported to HHS. Hacktivists tend to be motivated by political or social movements and protests. Given the increasing costs of healthcare in the U.S. and the recent Presidential elections where healthcare became a political battleground, we could start to see instances of hacktivist attacks in the near future. What remains unclear is whether these would show up on the HHS list, particularly if the goal is not to expose data but rather defamation of an organization. The CTAS “Cyber Threats to the United States Healthcare Sector” paper mentioned above contains a more in depth analysis of the hacktivism threat in healthcare.

Espionage is unsurprisingly low and is likely to remain this way within the HHS breach data. As noted in the “Cyber Threats to the United States Healthcare Sector” paper, espionage actors are primarily motivated in stealing intellectual property, not PHI. Further, the typical high level of sophistication of these attacks suggests healthcare organizations may not discover the attack for some time or perhaps not at all, and thus go unreported. Of the espionage attacks identified, all are loosely related to the incident affecting Triple-C and multiple insurance and government agencies in Puerto Rico.

Cybercrime actors are now and will likely continue to be the largest hacking threat to the healthcare industry for the foreseeable future. These actors are motivated by accessing and stealing data for the purposes of fraud (e.g., fraudulent reimbursements from Medicare/Medicaid), selling information on the black market, or ransom. While this presents the largest category of hacking threats according to the HHS data, these attacks are still minimal when compared to other types of breaches. This may be due to a number of factors.

First, cybercrime is global and typically cybercriminals search out targets of opportunity. In reviewing the global map of breaches on datalossdb.org, Canada, Australia, U.K. and parts of Asia are all hotbeds of activity, which may reduce what we see reported in the U.S. and more specifically by HHS. Second, cybercrime does not solely rely on breaches of healthcare data. Breaches can and do occur within healthcare organizations that do not affect healthcare data. Less we forget, healthcare organizations also hold troves of demographic and financial information that is itself valuable. Unless a breach includes PHI as defined by HIPAA, a healthcare institution would not have to report it under HITECH
(though we would likely still find out about it through the many state notification requirements that apply more broadly to personal information). Finally, isolated or limited incidents of medical identity theft may not be publicly reported because the breaches are less than 500 records. In the “Cyber Threats to the United States Healthcare Sector” paper many documented incidents of medical identity theft involved the information of only one individual. While still breaches, these would be included in the annual summaries provided to HHS, which unfortunately are not widely available.

**Unauthorized Access / Theft**
The primary difference between hacking and unauthorized access/theft in intentional breaches of PHI is the source of the threat vector: insider versus outsider (unauthorized access and theft have been grouped for this purpose in the context of this analysis). While all hacks were due to outsiders to the organizations breached, all but three unauthorized access/theft breaches were due to insiders. Of the three outliers, two were caused by an outsider accessing paper records and the other could not be determined.

The list below profiles some of the intentional unauthorized access breaches:

- A former employee of the South Carolina Department of Health and Human Services transferred the personal information of more than 228,000 Medicaid beneficiaries to his personal email and at least one other party.
- Two University of Miami Hospital employees were accessing patient information inappropriately and may have sold the information. The information was contained on “face sheets,” which are documents related to the patient registration process.
- Bruce Peller, who lost the Democratic primary for the 5th Congressional District seat, is accusing his former campaign manager, Christopher Church, of stealing information on about 10,000 current and former patients from a computer at Peller’s dental practice. Church fired back, accusing Peller of emailing him the information and telling him to call the patients to support his congressional campaign, which Peller disputes.
- A newly hired employee of Premier Imaging impermissibly took patient registration documents home with PHI on over 551 individuals. The information at issue included names, addresses, birth dates, social security numbers, and driver’s license numbers. As a result, the employee was terminated.
- Over 12,000 patients’ records were viewed for longer than one second by a Florida Hospital employee. Each patient was involved in a motor vehicle accident with many reporting that within days after being seen in the emergency room, they received solicitation calls asking if they needed a referral to a lawyer or chiropractor.
- Two employees of Memorial Healthcare System stole customer information with the intent of filing fraudulent tax returns.
- 8,000 students at the University of Pittsburgh Student Health Center had their protected health information stolen and later destroyed by an employee.

Across all incidents in this category, the data from HHS provides some indication of what motivates employee misconduct:
• 11% involved employees stealing or accessing records with the intent of filing fraudulent tax returns.
• 15% involved employees stealing records for their personal use, for example in the case of Peller stealing records to get contact information of individuals to support him in his political campaign.
• 15% involved employees stealing records to sell, with two instances of the buyers being attorneys.
• 55% involved the theft or unauthorized access of records for an indeterminable reason. These cases may be due to employees acting out against their employers for some wrong, or if more information were available may reveal intentions more closely related to those listed above.

One outlier was noted. In this instance, the employee was using the PHI of patients to gain access to controlled substances.

For the data we had available, money appears to be a primary motivator of employees. Over a third of the breaches involved the exchange of information for money or would eventually lead to income in the case of tax fraud. It is also clear that employees often feel entitled to use the information the healthcare organization maintains for their own personal motivations. Whether these employees believe what they are doing is right or wrong is debatable, but it is likely that many un-reported breaches are occurring because of employees walking out with data against company policy. In the case of the unknowns, it is difficult to come to a definitive conclusion as to the employees’ motivations. In 26% of these cases, the breach involved a former or terminated employee, supporting the case for employees acting out because they feel they have been wronged by their former employer. In other instances however, true intentions simply may not have been disclosed but could very well tie back to money, personal use, or retaliation.
In Conclusion

A review of the data of breaches affecting over 500 individuals compared with the same analysis one and two years ago reveals little change has occurred in the healthcare industry overall. In the coming year, we are likely to continue seeing approximately 35 breaches reported per month on average, down only slightly from 2011 and 2010.

Theft of devices will continue to lead as the cause of breaches, expanding from just laptops and mobile media to all endpoints. We believe the direction Stage 2 meaningful use is headed in requiring encryption or requiring a risk analysis as to why data is not encrypted is well founded because of this. HITRUST plans to take a similar stance in the 2013 HITRUST CSF and CSF Assurance Program.

Business associates have and will continue to be a significant source of breaches. This analysis has revealed that they are increasingly to blame for large losses of data, accounting for over 50% of the data breached to-date. While in theory the expansion of HIPAA should address this issue, in reality we have seen little change year after year across all organization types.

While we expect security to be a challenge for physician practices and even hospitals given the difficult environment these organizations operate within, we are surprised by the fact that government institutions in general and government agencies in particular have experienced the number of breaches that have been reported. These organizations should be some of the most well-equipped to protect confidential information and most well-informed on the areas of exposure, yet they remain a leading source of breaches making it difficult for regulators to “lead-by-example.”

But why are we seeing these trends? Why is theft such a prominent cause of breaches? Why have government agencies become a leading type of organization that experiences breaches? We believe the truth lies in the un-reported and under-reported data—the 57,000 breaches involving fewer than 500 individuals, the countless number of breaches that are not detected, not determined to be a breach due to a lack of harm, or simply not determined to be a breach due to a lack of education.

Based on what we know about healthcare organizations, our intuition would lead us to believe that data is leaking from the organization or is being accessed by unauthorized individuals on a daily basis. In a report from the Office of Management and Budget Medicare fraud in 2010 is estimated at $47.9 billion. The estimated value of a healthcare record is 50 times that of credit card information on the black market ($50 versus $1 per record). From technical security scans we know malware to be present on over 30% of home and small office computers. Physicians are known to take data home with them, store data on personal devices, and share passwords with administrators and nurses; we have seen little adoption of multi-factor authentication in hospital environments to mitigate these threats. We also know that the EHR and other clinical technology implemented at healthcare organizations are often rife with vulnerabilities that are not disclosed by the vendors making mitigation increasingly difficult.

But the data reveals that hacking incidents are only 6% of those reported, averaging two-to-three per month and malware comprise only 2% of breaches (compared with 22-23 thefts per month). It would seem if a breach in this area occurred, it is likely to affect more than 500 records. So is it an
identification challenge? Do organizations just not know they are being hacked? Of the hacking incidents reported, 72% were reported as detected within 30 days of the incident, with only 18% taking between three and 12 months to identify. It is possible there are just as many that have yet to be identified; that crime still focuses on non-healthcare data such as personally identifiable information (PII), financial data, and user credentials; or there is still an untapped market for cybercriminals that remain focused on retail and financial services industries.

It is this disconnect between what we know from other sources and hear from leaders in the industry, and what the HHS breach data say that leads us to believe that the number and types of breaches being reported is not entirely representative of what is actually occurring. The types of breaches referenced above are difficult to identify, often rely on self-reporting by the insider, and in some instances may only affect a small number of records per breach. While it is difficult to conclude the true nature or extent of breaches in healthcare, given the cyber threats that the industry faces we believe it must be taken seriously.

**Recommendations**

Based on the data, we believe organizations should be doing the following immediately:

**Endpoint Security**

- **Know your devices**
  - Ensure the organization has an effective way to inventory the endpoint devices its employees use that may contain sensitive information such as PHI.
  - Develop processes and procedures to support the organization’s “bring your own device” (BYOD) policies. This includes limiting the use of personal laptops and desktops unless explicitly authorized, and implementing technological restrictions for mobile media (e.g., USB drives, external hard drives, CDs/DVDs), mobile phones and tablets.

- **Protect your email**
  - Email is everywhere and employees want it that way, but the organization must ensure that email on devices not owned and controlled by the organization is limited in functionality (e.g., restricting the downloading of attachments) and is always accessed over a secure connection.
  - On mobile phones and tablets, require and implement encryption of the email clients (implementing third party email applications where necessary) to secure sensitive emails and attachments if the device is lost or stolen. Part and parcel with this is requiring passwords and inactivity timeouts to automatically secure the device after a specified period of idle time, typically two minutes.

- **Encrypt, encrypt, encrypt!**
  - Encrypt every device that can be easily carried. This includes the obvious mobile computing devices like laptops, but should also
extend to desktops. Desktops are the second most stolen device type behind laptops, and encryption is the only reliable way to prevent a breach.

- For less mobile endpoints like network servers, ensure they are physically secured, locked in cages and in secured areas that have limited access. Encryption should still be considered, particularly for those organizations looking at Stage 2 meaningful use criteria. If encryption is not applied, ensure there is documentation of the risk analysis, risk acceptance, and the mitigating controls in place.

Mobile Media Security

- Restrict the use of unencrypted mobile media, the third most stolen form of PHI and the most lost. Technical restrictions can be applied so that only select, authorized, encrypted USB devices can be used. These restrictions can be similarly applied to optical media such as CDs and DVDs.

- Don’t forget backup media! Tapes and other media used to backup data should be encrypted, always. Even if the organization uses a trusted third party to store and archive backups, all new tapes should be encrypted. For old media, conduct a risk evaluation to identify the time and cost of encrypting the media compared with the risk of it being lost or stolen. Ensure documentation is maintained of the risk evaluation if the organization decides not to retroactively encrypt backups.

Paper Records

- Transitioning paper records to electronic form can be a massive undertaking for organizations. Often this involves scanning each record or transcribing the information onto a computer. Ensure the organization has defined processes to track, store, and transport records to maintain the necessary levels of security. This includes identifying temporary, secure storage locations, documenting a chain of custody, and providing adequate means of secure disposal.

- Ensure employees are aware of proper handling procedures. This includes never leaving paper records unattended prior to them being properly secured. Paper records (laptops and briefcases too) should always be taken out of cars when possible or put into trunks where they are not visible. Onsite, records should never be left on
desks, copiers, scanners or fax machines.

- Ensure shredding is performed on-site if at all possible. If not possible, review and audit the shredding contractor’s processes and procedures to ensure trash is protected from on-site pickup to off-site destruction. Ensure destruction meets federal and/or state guidelines for destruction.

- Whenever possible, paper records should be centrally stored and managed within the facility. Just as technical controls are more manageable through a centralized console, paper records can be more easily protected in a single, secured location.

- Don’t forget the layered security model. Particularly for old, archived, and infrequently used records, secure them in locked cabinets in similarly locked, restricted rooms.

- Whether handled in-house or contracted through a third party service provider, locked bins for secure records disposal should be placed throughout the facilities. In placing bins, consider the number of users, facility layout (e.g., nurses stations, by printers/copiers/faxes), and times of year when volumes may increase.

- Ensure the bins are emptied regularly. In many cases organizations have secure disposal policies and bins placed throughout facilities. In areas where there is a high volume of paper waste, the bins can fill up quickly to the point where papers can no longer be deposited or, even worse, easily pulled out. A set frequency should be established, particularly if a vendor is utilized.

### Business Associates

- By now, all covered entities should have business associate agreements in place with their third parties, but having an agreement is not enough to effectively manage risk. Organizations must develop programs to manage third parties from before the contract is signed to after contract termination, and embed security evaluations along the way.

- For new and existing business associates, reduce the program’s burden by classifying each business associate based on its impact to the business and likelihood of a breach (i.e., risk). Appropriate classification (e.g., tier 1, 2, 3; high, medium, low) will allow the organization to focus its energy on those high risk business associates rather than casting an ineffectively wide net.
• Existing business associates should be re-evaluated periodically, but no less than once every three years depending on the classification and results of the evaluation (e.g., when security issues are known or become known).

• Require independent evaluations of security to transfer the burden of security to the business associate. HITRUST certifications, ISO certifications, or SSAE 16 reports among others can be requested to reduce the time and cost of reviewing the business associate’s security.

• Business associates are responsible for a majority (58%) of the healthcare records that have been breached since 2009. By evaluating, documenting and restricting access to only the data and systems required to conduct business, organizations can limit the impact of a breach involving a business associate. Your HIPAA Privacy Officer will be happy too!

Awareness for Physician Practices

• Entities that connect directly or indirectly with physician practices, particularly smaller ones, should treat these organizations as high risk and act accordingly.

• Just like business associates must provide assurance that controls are in place, so should physician practices. While obtaining a certification or SSAE 16 from a small physician practice is unlikely, large organizations should perform basic reviews of the security practices of their affiliated or connected physician practices. This may include directing the physician practice to resources like the HITRUST to fill out a simplified self-assessment for small organizations focused on key technology controls (e.g., anti-malware, firewalls, and encryption)\textsuperscript{xxi}.

• If a practice has one or more individuals that manage information technology (IT) resources, determine if they are taking the necessary precautions to secure sensitive information. Areas of focus include:
  o Information Security Policies/Procedures
  o Endpoint Security (including laptops, desktops, servers, phones, and tablets)
  o Mobile Media Security
  o Wireless Security
Leverage existing resources

- Ensure a risk assessment has been performed within the past three years, even if it was performed internally, that addresses the above-listed areas.
- Practices should reach out to legal counsel and request guidance on the organization’s HIPAA security, privacy and breach programs. If counsel cannot provide direct assistance, they likely can provide a reference to reputable professionals who can.
- There are a number of tools, websites and organizations that provide guidance, templates and other resources to get up to speed on HIPAA and ensure a Physician Practice is secured:
  - HHS Security Rule Guidance\textsuperscript{xxii}
  - Regional Extension Centers\textsuperscript{xxiii}
- The HITRUST CSF Assurance Program\textsuperscript{xxiv} provides a simple process and tool to conduct a self-assessment of a practice’s security. The Office for Civil Rights (OCR) has an audit guide\textsuperscript{xxv} and the National Institute for Standards and Technology (NIST) has a toolkit\textsuperscript{xxvi}, which may also be used in conducting self-assessments.

Healthcare organizations that have addressed most or all of these key areas should begin to look ahead at the risks that may be coming. This includes minimizing the risk of internal and external compromise by instituting rigorous human security policies (for current and former employees/contractors and for patients/customers) and employing technical security solutions such as Data Loss Prevention (DLP) and Intrusion Detection/Prevention Systems (IDS/IPS).

Note, these recommendations should not be construed as a plan for a comprehensive security program; instead, they provide strong starting points for security initiatives based on lessons learned from three years of healthcare breach data.
How HITRUST Is Adapting

Since the release of the HITRUST CSF Assurance Program, HITRUST has analyzed and considered HHS and other breach data to help determine our certification requirements. Our position has always been to provide a reasonable starting point for healthcare organizations with a focus on the high risks. Over time, we believe we can facilitate a fundamental shift in the industry towards one that is security and privacy conscious on par with other leading industries.

In line with this, we conduct this analysis periodically and make it freely available not only to keep the industry apprised of trends, but to inform the industry about modifications to our own programs and requirements. Below is a summary of things we have recently done or are planning to do in light of this information:

- The HITRUST Common Security Framework (CSF) continues to be reviewed, refined, and updated to account for the issues leading to healthcare breaches. HITRUST’s goal for the industry with the CSF is to not only provide organizations with a common, comprehensive set of security controls that reference to applicable standards and regulations, but to ensure that organizations adopting the CSF are not prone to frequent and high impact breaches. This includes:
  - Adjusting the CSF’s level requirements to ensure fundamental risks, such as endpoint device and mobile media encryption, that affect all organizations regardless of size and sophistication can be identified and protected against.
  - Prioritizing high risk issues for certification to focus assessment and remediation efforts based on the most likely areas to result in a breach. (HITRUST believes the CSF is currently very strong in this regard, but will be adding key requirements related to security program governance to ensure the focus is not just on the controls, but the management of controls.)
  - Adding security requirements for new and updated authoritative sources to the CSF for 2013, including NIST SP 800-53 R4, CAQH CORE, TX HB 300, and meaningful use Stage 2.
- The CSF Assurance Program is being updated to fully address the HIPAA Security, Privacy and Breach Notification rules, align with Stage 1 and 2 meaningful use requirements, and provide adequate coverage for high risks including endpoint security, mobile media security, third party assurance, and continued requirements for secure disposal.
- The CSF Assessment Tool, which organizations use to conduct self- and third-party assessments under the CSF Assurance Program, is being updated to simplify the security control questions and provide better recommendations to organizations. This will enable organizations of all types, sizes and complexity to effectively utilize the toolkit in conducting accurate and reliable risk assessments for HIPAA, meaningful use, and third party business requirements.
- HITRUST is developing and will be releasing detailed illustrative procedures aligned with the certification criteria to provide standardized, industry-approved audit and assessment guidance to HITRUST CSF Assessors, covered entities and business associates.
• HITRUST recently released its Cyber Threat Analysis Service (CTAS) which provides monitoring of specific healthcare data threats, allows for proactive vulnerability reporting and knowledge sharing, and supports best practices to mitigate these risks.

About HITRUST

The Health Information Trust Alliance (HITRUST) was born out of the belief that information security should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST, in collaboration with healthcare, business, technology and information security leaders, has established the Common Security Framework (CSF), a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal health and financial information. Beyond the establishment of the CSF, HITRUST is also driving the adoption of and widespread confidence in the framework and sound risk management practices through awareness, education, advocacy and other outreach activities. For more information, visit www.HITRUSTalliance.net.
All breaches involving unsecured and unprotected PHI must be reported to HHS regardless of the size of the breach. Breaches under 500 records at this time are not publicly disclosed and are only required to be reported to HHS in sum per organization annually. According to a presentation delivered by OCR in May, 2012, over 57,000 breaches involving fewer than 500 records have been disclosed to HHS since the breach notification rule went into effect.


The projected values for 2012 are based on the number of breaches as calculated through a linear forecast of the data through. The linear trendline is based from Q3, 2009 through the actual data of Q2, 2012, and forecasting the third and fourth quarter of 2012. Since many of the forecasts result in fractions of whole numbers, we have rounded the estimate to the nearest whole number.


A survey by SK&A estimated that 46% of practices had adopted an EHR as of January 2012, compared (http://www2.idsexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Sudy.pdf). This was compared with the CMS active registrations (see endnote x) which states 303,072 eligible professionals have registered with CMS. Out of the total number of physicians in the United States (see endnote xii) we arrived at 47.5% giving us a range for adoption.

A data brief from ONC in February 2012 estimated EHR adoption of hospitals at 34.8%, which was an 82% increase from 2010 to 2011. We assumed linear growth from 2011 to 2012 to arrive at 63.3% adoption in 2012 (http://www.healthit.gov/media/pdf/ONC_Data_Brief_AHA_2011.pdf). This was compared with the CMS active registrations (see endnote x) which states 4,057 hospitals have registered with CMS. Out of the total number of hospitals in the United States (see endnote xi) we arrived at 73.2% giving us a range for adoption.

HITRUST C-TAS is a joint venture between the HITRUST Alliance and ISIGHT Partners. For more information, please visit http://hitrustralliance.net/ctas/.