The School of Hard Knocks
Extended Version

Lessons Learned from a Medical Practice Data Breach
Brian J. Courtney, RPLU, AAI

Brian Courtney joined The Safegard Group, Inc. in April 2005 and serves as a Producer and the Healthcare Practice Leader for the company. He is primarily responsible for the direction of client services to the healthcare industry.

Brian began his career at the height of the medical malpractice crisis. Working with a large regional insurance broker, Brian served with the healthcare practice leader helping hospital systems and physician groups obtain medical malpractice coverage.

Prior to joining The Safegard Group, Brian joined a large national insurance brokerage firm where he gained considerable experience in healthcare risk management serving the needs of large physician groups, long-term care facilities, home healthcare providers, and allied health professional organizations.

Currently, Brian is helping many of his clients with Risk Management initiatives, such as Risk Assessments, Incident Response Planning, Contractual Risk Transfer, Insurance Protection and a host of other related services.

Brian lives in Downingtown, Pennsylvania with his wife Erin and three kids, Aidan, Carter & Chase. He is active in the community volunteering his time with the Lionville Youth Soccer Association and Brandywine Health Foundation. He is also an fitness/health enthusiast recently competing in the Spartan Races, which was voted the 2012 Best Obstacle Course Race by Outside magazine.
Agenda

- The painful truth about healthcare, medical identity theft and data breach risk.

- HIPAA – The Standard of Care in Malpractice Claims

- Lessons learned from an actual data breach involving a medical practice

- Risk Management Strategies to Reduce a Similar Fate
“We expect healthcare breaches will increase – both due to potential economic gain and digitization of records . . . Healthcare organizations face the challenge of sensitive information stored on their network, which combined with the value of a medical identity string makes them an attractive target for cyber criminals. The problem is further exasperated by the fact that many doctor offices, clinics and hospitals may not have enough resources to safeguard their patients’ PHI.”

Source: Experian 2015 Data Breach Industry Forecast
“Cyber attacks have expanded from a tech problem to a corporate-wide issue . . . business leaders are being held directly accountable for data breaches . . . scrutiny of corporate leadership’s management of security may continue to increase in the form of critical media coverage and legal and regulatory scrutiny in the wake of a major incident . . . senior executives will be expected to have a better understanding of the data breach response plan, comprehension of new technologies and security protocols in the workplace, and have a clearly-defined chain of response should a breach occur.”

Source: Experian 2015 Data Breach Industry Forecast
“a majority of companies will miss the mark on the largest threat, employees. Between human error and malicious insiders, time has shown us the majority of data breaches originate inside company walls. Employees and negligence are the leading cause of security incidents but remain the least reported issue.”

Source: Experian 2015 Data Breach Industry Forecast
Why Do They Think This?

What Does The Data Tell Us About Data Breaches?
Breaches by Type of Entity

Breaches by Type of Information

2014 Healthcare Providers Data Breaches by Type

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unintended Disclosure</td>
<td>17</td>
</tr>
<tr>
<td>Hacking or Malware</td>
<td>18</td>
</tr>
<tr>
<td>Insider</td>
<td>11</td>
</tr>
<tr>
<td>Physical Loss</td>
<td>18</td>
</tr>
<tr>
<td>Portable Device</td>
<td>17</td>
</tr>
<tr>
<td>Stationary Device</td>
<td>6</td>
</tr>
<tr>
<td>Unknown</td>
<td>2</td>
</tr>
</tbody>
</table>

Source: Privacy Rights Clearinghouse
Examples of Published Healthcare Data Breaches

**Hacking**
The office of Dr. Barry J. Snyder at Penn Highlands Brookville, a healthcare service provider for the Brookville area in Pennsylvania, notified patients of a data breach when a third party accessed the third party vendor's server who maintains records for Dr. Snyder.

**Unintended Disclosure**
Touchstone Medical Imaging notified patients of a data breach as a “result of an open share that was exposed to the Internet.”

**Insider**
NRAD Associates informed patients of a data breach to their system when a radiologist employed with the facility accesses patient information without authorization.
Average Records Per Breach by Type of Entity

- Corporate: 86,797 (FQA), 31,278 (Q2 2014)
- Education: 40,909 (FQA), 45,890 (Q2 2014)
- Government: 29,740 (FQA), 29,740 (Q2 2014)
- Healthcare: 20,175 (FQA), 20,587 (Q2 2014)
- Other: 18,210 (FQA), 20,587 (Q2 2014)
### Average Total Cost of Breach by Type of Entity

**Corporate**: $17,446,166
- **FQA**: $6,286,971
- **Q2 2014**: $11,159,195

**Education**: $9,223,823
- **FQA**: $8,222,703
- **Q2 2014**: $1,001,120

**Government**: $5,977,772
- **FQA**: $5,977,772
- **Q2 2014**: $563,805

**Healthcare**: $4,055,134
- **FQA**: $4,137,987
- **Q2 2014**: $82,853

**Other**: $3,660,210
- **FQA**: $2,561,783
- **Q2 2014**: $1,098,427

**Source**: Navigant Information Security & Data Breach Report, October 2014
The Value of Medical Identities & It’s Risk Impact on Healthcare Providers
The Value of a Medical Identity

The consensus of experts is that the value of medical identities is greater than Social Security numbers on the black market. A recent investigative reporter interviewed a medical identity theft middleman who confirmed this perception. Some estimates suggest that criminals are monetizing medical identities at a rate that is between 20 and 50 times more than financial identities. “A stolen medical identity has a $50 street value—whereas a stolen Social Security number, on the other hand, only sells for $1,” said Kirk Herath, Nationwide Chief Privacy Officer. “However, while most people are very careful with their Social Security number to protect their credit and personal information, they tend to be less careful when it comes to their medical information.”

Source: Medical Identity Fraud Alliance
Medical Identity Theft Base Rates

Source: Ponemon Institute Fifth Annual Study on Medical Identity Theft
2014 Reasons for Medical Identity Theft

- To Obtain Healthcare Services or Treatment: 59%
- To Obtain Prescription Pharmaceuticals or Medical Equipment: 56%
- To Obtain Government Benefits, Including Medicare or Medicaid: 52%
- My Healthcare Records Were Accessed or Modified: 23%
- The Thief Obtained Fraudulent Credit Accounts in My Name: 14%
- Don't Know: 5%
- My Credit Report Was Accessed or Modified: 5%

Source: Ponemon Institute Fifth Annual Study on Medical Identity Theft
What About The Soft Costs?
Embarrassment Due to Disclosure of Sensitive Personal Health Conditions: 89%
Loss of Career Opportunities: 19%
Termination of Employment: 3%
Other: 5%

Source: Ponemon Institute Fifth Annual Study on Medical Identity Theft
Did Healthcare Provider's Negligence Cause Medical Identity Theft?

- Yes, Very Likely: 32%
- Yes, Likely: 21%
- No, Not Likely: 9%
- No, Not Very Likely: 8%
- Can't Determine: 30%

Source: Ponemon Institute Fifth Annual Study on Medical Identity Theft
Did It Dimish Your Trust In Healthcare Provider?

- Significant Impact on Confidence and Trust: 50%
- Some Impact on Confidence and Trust: 35%
- No Impact on Confidence and Trust: 15%

Source: Ponemon Institute Fifth Annual Study on Medical Identity Theft
Attributes about Data Breach Notification

- Notification about data breach and the loss or theft of my personal information is relevant to me (85%)
- Organizations that fail to protect my personal information are untrustworthy (83%)
- The privacy and security of my personal information is important to me (82%)
- The data breach notifications I've received did not explain all the facts and "sugar coated" the message (58%)
- Organizations should inform me about a data breach only if they are certain I am at risk (57%)

Source: Ponemon Institute© Research Report
I will discuss how the breach was reported via email or social media

The organization reporting the breach is not to blame

I will discontinue (or already discontinued) my relationship

I will continue my relationship as long as it does not happen again

I might discontinue my relationship

Source: Ponemon Institute© Research Report
The Office of Civil Rights

What’s Their Position?
What Has OCR Said About Enforcement?

“This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented. These changes not only greatly enhance a patient’s privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates.”

Director OCR
Leon Rodriguez
Enforcement Results
January 1, 2013 through December 31, 2013

Total Resolutions 14,300
- Resolved after Intake and Review: 9,837 (69%)
- No Violation: 993 (7%)
- Corrective Action Obtained: 3,470 (24%)

Total Investigations 4,463
- 78%: 3,470
- 22%: 993

Source: www.hhs.gov/ocr
Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Issue 1</th>
<th>Issue 2</th>
<th>Issue 3</th>
<th>Issue 4</th>
<th>Issue 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Mitigation</td>
</tr>
<tr>
<td>2012</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Mitigation</td>
</tr>
<tr>
<td>2011</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Mitigation</td>
</tr>
</tbody>
</table>
HIPAA
The New Standard of Care?
What Is Medical Malpractice?

Definition:

The failure of a healthcare provider to meet the standard of care and degree of skill that other healthcare providers would use under similar circumstances.

Source: Professional Liability Underwriting Society
The Elements of a Valid Medical Malpractice Claim

Duty of Care (Patient – Provider Relationship)

Breach of Duty (Standard of Care)

Damages or Injury

Causal Connection (Breach of Duty & Damages)

Source: Professional Liability Underwriting Society
Omnibus HIPAA/HITECH Rule Defined

Definition:

An acquisition, access, use, or disclosure of protected health information in a manner not permitted

*Under HIPAA, no private cause of action is available to patients*
Recent Case Rulings

Hinchy v. Walgreens (Indiana)
Byrne v. Avery Center (Connecticut)
Hinchy v. Walgreens

- Audra Peterson worked as a Walgreen’s pharmacist which plaintiff Abigail Hinchy used.

- Audra Peterson learned of affair between her husband, Davion Peterson and Abigail Hinchy, which resulted in birth of a child.

- Hinchy demanded child support from Davion Peterson.

- In an effort to avoid child support, Audra Peterson accessed Hinchy’s prescription history and disclosed to her husband.
Hinchy’s Malpractice Case

_Duty of Care_
Hinchy was a Walgreen’s patient

_Breach of Duty (Standard of Care)_
Walgreen’s clearly violated HIPAA

_Damages or Injury_
Hinchy suffered emotional distress and mental anguish

_Causal Connection_
Hinchy’s damages were connected to HIPAA violation
Byrne v. Avery Center

- Byrne was a patient of the Avery Center and provided a copy of its privacy policy.
- Byrne specifically instructed Avery Center not to release medical records to her estranged father of her child.
- Estranged father filed paternity suit action against Byrne and Avery Center was served a subpoena for Byrne’s medical records.
- Avery Center mailed copy of medical records to court.
- Byrne suffered harassment and extortion threats after estranged father viewed medical record.
Byrne’s Malpractice Case

**Duty of Care**

Byrne was a patient of Avery Center

**Breach of Duty**

Avery Center should have received authorization from Byrne, obtained a protective order or filed a motion to quash

**Damages or Injury**

Byrne suffered emotional distress

**Causal Connection**

Emotional distress was caused by HIPAA Violation
Other Risk Factors

- Patient/Employees victims of retaliation
- Use of attorneys to collect delinquent payments
What Can We Learn From These Cases?

- States are beginning to allow HIPAA to establish the Standard of Care, opening the door for private right of action against healthcare providers.

- Leave open the possibility that an omission to safeguard EHR (i.e. encryption) would fall under the HIPAA Standard of Care ruling.
The School of Hard Knocks

Lessons Learned from a Healthcare Organization
The Backdrop

In January 2011, GetWell, a medical practice acquired FeelBetter, another medical practice. As a result of the acquisition, GetWell was tasked with migrating the electronic health records of FeelBetter into GetWell’s electronic health record system. The migration needed to be expedited quickly and despite the time crunch, the migration went as anticipated (or so they thought).

On February 5th 2011, the Director of IT for GetWell noticed some irregular activity.
Common Sense Finally Prevails

After a few days, the IT Director informs the GetWell management team of the suspicious activity. The management team decides to contact their corporate attorney, who is great in corporate law, but has no background in data breach legal law guidance. The attorney recommends that they contact their insurance agent for guidance as they currently purchase Cyber Security insurance. After a few more days pass, the agent locates an attorney who specializes in post-data breach law guidance and is available to assist them.

The agent advises the client that the attorney could be expensive than what they are accustomed to.
The Data Breach Coach

Not knowing the severity of the situation and reluctant to expend significant legal fees, GetWell relents and contacts the Data Breach expert on February 15th. After interviewing the management team regarding the strange activity on the company’s network, he recommends that they engage his services to help them through a possible data breach.

*The Cost of the Data Breach Expert’s services:*

$10,000
Data Breach Legal Law Guidance

Next Steps

- Hold call with Forensic IT firm to obtain the estimated cost for their services.
- Finalize the legal analysis
- Prepare the notification letters
- Engage a call center to obtain the cost for their services
- Write the Frequently Asked Questions for the website
- Engage a Notification vendor to obtain the cost for their services
- Engage an ID Fraud Remediation company to obtain the cost for their services
- Develop State AGs and Department of HHS notice
- Implement a litigation hold
Results of Forensic Investigation

On March 12\textsuperscript{th}, GetWell engaged a Forensic IT investigation firm. During the investigation, it was discovered that FeelBetter was hacked prior to their acquisition. The hacker created a “backdoor” to the system, which allowed them access to the PHI of 300,000 patients of GetWell. The PHI included but was not limited to Names, SSN, Medical ID numbers, and Credit Card Numbers.

The Cost of the Forensic IT investigation & Security Remediation:

$90,000
The Next Round of Forensic Investigation

Because Credit Card numbers were obtained, further forensic investigation needed to be done which was PCI specific.

On March 31st, GetWell engaged another Forensic IT firm to conduct the PCI specific investigation.

**The Cost of the Investigation & Remediation:**

$100,000
Notification Begins . . .

On April 7\textsuperscript{th}, after approximately two months since discovery of the data breach, the legal expert has negotiated and executed the Pre-Notification with the FAQ. Letters were scheduled to be sent from April 7\textsuperscript{th} to June 7\textsuperscript{th}.

\textit{The Cost of Hiring the Notification Vendor:}

$300,000
Who Do I Call?

At the same time the legal expert was negotiating with the notification vendor, they also provided a number for the affected parties to call with questions. In order to handle the anticipated influx of calls, a Call Center was established.

*The Cost of the Call Center:*

$26,250
Let’s not forget PR

The legal expert also recommended hiring a Public Relations firm to become the spokesperson for the Data Breach. They placed a full-page ad in the Philadelphia Inquirer and also prepared a statement on GetWell’s website.

The Cost of the Public Relations firm:

$21,000
Oh, and one more thing . . .

Within the notification letter, the legal expert suggested GetWell provide to provide those affected a free year of ID monitoring and fraud remediation services.

The Cost of ID Monitoring & Fraud Remediation:

$1,050,000
But wait there’s more

On April 21st, the Attorney General conducts their own investigation. With the support of the legal expert, GetWell provides the AG the information they need to conduct their investigation.

As a result of the investigation, the AG levies a fine of:

$500,000
Class Action Filed

On January 14, 2012, a year after the breach was discovered, a class action lawsuit was filed against GetWell for not taking the proper precautions to securing the data information systems. Legal counsel was obtained by GetWell to handle the eDiscovery, as well as, the defense of the class action. As a result, damages were limited to ID Fraud Remediation and Credit & Health Record monitoring, which was already provided.

The Cost of eDiscovery Litigation and Legal Defense:

$393,750
GetWell Data Breach Total Damages

Data Breach Law Legal Guidance: $ 10,000
Forensic Investigation/Remediation: $ 90,000
PCI Investigation/Remediation: $100,000
Customer Notification: $300,000
Call Center: $ 26,250
Credit Monitoring: $750,000
ID Fraud Remediation: $300,000
Public Relations Service: $ 21,000
State AG Fines: $500,000
eDiscovery Litigation: $300,000
Legal Defense & Damages: $ 93,750

TOTAL: $2,481,000
Risk Management Strategies

Simple Solutions for Healthcare Organizations
Where Are Most Healthcare Organizations Falling Short?

- Risk Assessments are not conducted for potential vulnerabilities
- Password protections weak and/or accessible
- Encryption on Mobile Devices such as laptops and smart phones
- Business Associate Agreements does not shift risk towards nor allow for subrogation against the BA for their negligence.
- Data Breach Incident Response Planning not detailed or thought out.
- Insurance policies do not provide any or enough coverage in the right areas.
Risk Assessment

- Security Policy
- Security Organization
- Information & Asset Classification
- Personnel Security
- Physical & Environmental Security
- Communications & Operations Management
- Access Control
- Systems Development & Maintenance
- Business Continuity & Management
- HIPAA/HITECH Compliance
- Privacy

Source: NetDiligence
Passwords

• Passwords are often used to protect access to secure files or sensitive information (however, they don’t protect as well as encryption)
  • How many times have you seen someone’s password on a sticky note attached to a computer monitor?
  • The problem is that they are only as good as the person who created it
• According to a recent Imperva study involving a data breach of 32 million passwords, the most common password is . . .

Source: PCworld
## Password Popularity - Top 20

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
<th>Number of Users with Password (absolute)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>290731</td>
</tr>
<tr>
<td>2</td>
<td>12345</td>
<td>79078</td>
</tr>
<tr>
<td>3</td>
<td>123456789</td>
<td>76790</td>
</tr>
<tr>
<td>4</td>
<td>Password</td>
<td>61958</td>
</tr>
<tr>
<td>5</td>
<td>iloveyou</td>
<td>51622</td>
</tr>
<tr>
<td>6</td>
<td>princess</td>
<td>35231</td>
</tr>
<tr>
<td>7</td>
<td>rockyou</td>
<td>22588</td>
</tr>
<tr>
<td>8</td>
<td>1234567</td>
<td>21726</td>
</tr>
<tr>
<td>9</td>
<td>12345678</td>
<td>20553</td>
</tr>
<tr>
<td>10</td>
<td>abc123</td>
<td>17542</td>
</tr>
</tbody>
</table>
Encryption

• Mobile devices like laptops should have hard disk encryption enabled.

• All wireless devices should use superior form of encryption scheme like Wireless Protection Access (WPA) or WPA2 and not (WEP or LEAP) which can be easily compromised.

• If data is encrypted, generally there are no reporting obligations. Take advantage of the safe harbor provision by encrypting all records.

• However, some states require the use of at least 128-bit encryption to protect any personal data in transit including information sent via e-mail, laptops, external hard drives, USB memory sticks, CDs, etc. 

Source: PCworld
Business Associates

- Enforce security standards for third parties that connect to your network. If so, are:
  - Clearly manage and document compliance of business associates and their sub contractors
  - Requests for third party connectivity reviewed and approved by management
  - Technical risk assessments performed on third parties prior to approval
  - Third party connections monitored for security events
- Third party contracts include security provisions. If so, do the contracts include:
  - A service level agreement that specifies security requirements and responsibilities.
  - Provisions for compliance with applicable regulations (i.e. HIPAA and HITECH).
  - A right to audit clause.
  - Procedures for escalating security related events.
Data Breach Incident Response Plan

- Build Your Team
- Implement a Process
- Communication Plan
- Readiness
- Simulate
- Improve
Caveat Emptor

Insurance Buyer Beware

- Failure to Update Security Patch Exclusion
- Unencrypted Data Exclusion
- Mobile Device Exclusion
- Voluntary vs. Non-Voluntary Notification
- Credit Monitoring Services vs. All Monitoring Services
- Dishonest, Fraudulent Criminal/Intentional Acts, except for Rogue Employees.
Next Steps

- Do a gap analysis/risk assessment of your HIPAA privacy and security, data breach compliance processes and procedures
- Prepare a data breach response team, form letter, form press release
- Develop a breach analysis tool and log to track decision making process
- Educate all workforce members, at least annually
- Revise BA Agreements
- Consider purchase of Cyber Risk insurance and the coverage considerations that are meaningful to healthcare risk.
Questions???
Contact Information

Brian J. Courtney, RPLU, AAI
Healthcare Practice Leader
The Safegard Group, Inc.
100 Granite Drive, Suite 205
Media, PA 19063
610.892.6812 (O)
610.420.1920 (M)
bcourtney@safegardgroup.com