The Top 10 HIPAA Compliance Fails
Lessons Learned For 2018
TABLE OF CONTENTS

Introduction ......................................................................................................................................................2
The Most Significant HIPAA Enforcement Actions in 2017 ..................................................................................3
The Top Ten Healthcare Compliance Fails and Lessons Learned ........................................................................4
What Are the Compliance Benefits of Cloud Fax? .................................................................................................8
What is the Cloud Fax Business Model? ...........................................................................................................8
Why Healthcare Providers Choose eFax Corporate ............................................................................................9
INTRODUCTION

As businesses embrace digitization — and the Internet of Everything (IoE) begins to take shape — defenders of corporate data will have even more to worry about. The attack surface will only expand, giving adversaries more space to operate. And end users are, as they've always been, the weak link in the security chain.

For healthcare providers, from a small physician practice to the largest hospitals, there are serious consequences a covered entity faces when it suffers a data breach — specifically the potential for regulatory penalties and other negative impacts such as lost business resulting from all the negative publicity.

THE SOURCES AND CAUSES OF DATA BREACHES

Turning now to the most common sources of large healthcare data breaches, this chart is pretty self-explanatory. Large means greater than 500 records.

One thing should leap out at you — in an era of rapid migration to electronic medical systems, don't forget about paper records! The OCR reports that paper is still an area where they see a lot of complaints because people forget about protecting them, especially at the Business Associates — so you need to be aware of what your business associates are doing with paper records, and how those records are disposed of.

Don't be the subject of a news story in the local newspaper about boxes of medical records found in a dumpster containing the personal information of thousands of your patients. You can be sure the government will want to know how they got there.

You can also see the prevalence of portable devices and laptops, with a combined total of 26%, is the single largest source of data breaches.

And that should come as no surprise – if you allow ePHI to be stored on movable devices, sooner or later it will walk away and be lost or stolen. And if the data on that device not encrypted, you will have a reportable data breach to deal with.

Looking now at the most common causes of data breaches, this chart is also self-explanatory. A couple of points are worth noting.

First, Theft and loss of devices accounts for nearly half of the reported incidents, or 48%. So if you are still putting ePHI on movable devices, expect them to get lost or stolen, and plan accordingly.

This percentage has come down a bit since last year so maybe people are getting more conscientious about locking things up? Or maybe more devices are encrypted which would remove them from the reportable data breach category? Both things would be positive developments.
However, if this chart were based on the total number of individuals affected, almost the entire chart would be purple, because it is cyber-hacking that affects the vast majority of records breached and individuals affected, but only about 17% of the actual incidents.

So, the next highest after theft and loss is Unauthorized Access or Disclosures at 27%. The point is that these are mostly related to internal management of people, not to outside hackers operating out of some foreign country. That means it is under your control as a healthcare provider or business associate to do something about it.

The important takeaway is that while cyber-hacking is responsible for most of the very large data breaches, it is not the most likely event to impact your organization, especially for the majority of smaller providers.

The position of the OCR is that “While your risk landscape is huge and includes all the things [with ePHI] that can walk away from your facility, Cyber threats are a very small portion of that risk landscape.”

So plan and prepare accordingly

**2017 HIPAA ENFORCEMENT ACTIONS**

In addition to its audit program, the OCR investigates complaints and reported data breaches. Let’s review the more significant breaches of PHI that resulted in significant penalties during the previous year, and then we will examine the lessons that were learned.

Let’s now take a look at the top five settlements in 2017, and a couple of smaller ones.

**Memorial Healthcare System** at $5.5 million dollars is the largest of the year and involved access of ePHI by staff who were not authorized to do so, and also the lack of audit controls to keep track of that type of behavior. This one ranks among the largest settlements, ever.

<table>
<thead>
<tr>
<th>Major HIPAA Settlemets In 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Memorial Healthcare System – $5.5 million</td>
</tr>
<tr>
<td>2. Children’s Medical Center of Dallas- $3.2 million</td>
</tr>
<tr>
<td>3. CardioNet – $2.5 million</td>
</tr>
<tr>
<td>4. Memorial Hermann Health System – $2.4 million</td>
</tr>
<tr>
<td>5. 21st Century Oncology – $2.3 million</td>
</tr>
<tr>
<td>6. MAPFRE Life Insurance Co. of Puerto Rico – $2.2 million</td>
</tr>
<tr>
<td>7. Presence Health – $475,000</td>
</tr>
<tr>
<td>8. Metro Community Provider Network – $400,000</td>
</tr>
<tr>
<td>9. Luke’s-Roosevelt Hospital Center Inc. – $387,000</td>
</tr>
<tr>
<td>10. Center for Children’s Digestive Health – $31,000</td>
</tr>
</tbody>
</table>

Second was Children’s Medical Center, $3.2 million, stemming from an investigation of data breaches as far back as 2009 and again in 2013. The violations included compliance with the Security Rule and a failure to implement adequate corrective measures over a number of years.

**CardioNet**, the next highest at 2.5 million, involved the theft of an unencrypted laptop containing ePHI, and the subsequent investigation revealed the lack of an adequate risk assessment. Sounds familiar, doesn’t it?

4th is Memorial Herman, at $2.4 million, in which the name of a patient who was arrested for presenting fake identification was revealed in a press release and in subsequent interviews with the media and others.

This seems to fall under the category of “what were they thinking? However, the actual rule violation was obviously, the unauthorized disclosure of PHI.

**21st Century Oncology**, at $2.3 million. Due to a lack of audit controls, the company did not know it had a data breach until the FBI presented over 2.2 million patient records purchased by an informant. Those patients have filed a class action suit against the company, which was already in bankruptcy.
Also worthy of note is the St. Lukes case, because this mistake cost the New York hospital $387,000 for sending two faxes--yes faxes--revealing patients’ HIV status to their employer instead of their health plan.

Now for the smallest -- the settlement with Children’s Digestive Health, at a mere $31,000, is there to prove a point. The violation involved lack of a BAA, but the real point OCR was trying to make is, “no company is too big, or too small, to escape compliance enforcement.”

TOP 10 LESSONS LEARNED FOR 2018

Now we will review the top ten issues that the Office of Civil Rights of the Department of Health & Human Services (OCR) selected for awareness of because of the number of enforcement actions in every one of these areas. Keep in mind, the following issues were hand-picked by the top officials responsible for overseeing HIPAA compliance and enforcement. So you can bet that these areas will continue to receive heightened scrutiny going forward in 2018.

**Issue #1: Affirmative Disclosures Not Permitted**

See 45 C.F.R. §164.502(a) -- The Privacy Rule provides that “Covered Entities or Business Associates may not use or disclose PHI except as permitted or required.”

Examples of Actual Violations:

- Covered Entity permits news media to film individuals in its facility prior to obtaining their authorization.
- Covered Entity publishes PHI on its website or social media without authorization by the individual(s). This can include testimonials or even pictures of happy patients.
- Covered Entity confirms that an individual is a patient and provides other PHI to reporter(s) without authorization from the individual.
- Covered Entity faxes PHI to an individual’s employer without authorization.

**Issue #2: Lack of Business Associate Agreements**

See 45 C.F.R. §164.308(b) – HIPAA requires that covered entities enter into agreements with their business associates to ensure they will appropriately safeguard protected health information.

Here are a few examples of potential Business Associates:

- A collections agency providing debt collection services to a health care provider which involves access to protected health information.
- An independent medical transcriptionist that provides transcription services to a physician.
- A subcontractor providing remote [cloud] backup services of PHI data for an IT contractor-business associate of a health care provider.

The OCR is still seeing organizations exchanging ePHI with business associates without a signed agreement (BAA), which indicates a real need for education.

Remember, if a provider or covered entity exchanges ePHI with a third party, that 3rd party becomes a business associate regardless of whether or not there is a signed agreement. And lack of a signed agreement with a BA is a HIPAA violation.

The OCR pointed out a few examples involving a debt collection agency, a medical transcriptionist, and a cloud back up provider.

According to their guidance on Cloud Service Providers, the rule is if you create, maintain, receive or transmit ePHI, on a more than temporary basis, you will need to have a BAA with the covered entity that is providing the ePHI.

A cloud storage provider, for example, obviously is not a simple “conduit” for information because they typically store ePHI on a more than temporary basis. Maintenance of this data is ‘prolonged,’ and so a BAA is required.
Issue #3: Incomplete or Inaccurate Risk Analysis
See 45 C.F.R. §164.308(a)(1)(ii)(A) – “Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information....”

- Organizations frequently underestimate the proliferation of ePHI within their environments. When conducting a risk analysis, an organization must identify all of the ePHI created, maintained, received or transmitted. Lack of an adequate Risk Assessment as required under HIPAA.

This issue comes up a lot. In fact, the problems with ePHI proliferating throughout an organization in various devices and systems where it may not be properly accounted, is not new, and there are many places that ePHI can hide and come back to bite you.

Examples: Applications like EHR, billing systems; documents and spreadsheets; database systems and web servers; fax servers, cloud servers; medical Devices; messaging apps, media, transcriptions, etc.

Issue #4: Failure to Manage Identified Risk
See 45 C.F.R. §164.308(a)(1)(ii)(B). The Risk Management Standard requires “…security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the Security Rule].”

- Investigations uncovered that risks attributable to a reported breach had been previously identified as part of a risk analysis, but that the organization failed to act on its own risk analysis and did not implement appropriate security measures.

- In some instances, encryption was included as part of a remediation plan; however, activities to implement encryption were not carried out or were not implemented within a reasonable timeframe.

The requirement for risk management follows from the risk analysis. Once the threats to ePHI are identified by the risk analysis, it is incumbent upon the provider to actually do something to address the risks identified by the risk analysis, and do so within a reasonable amount of time.

The OCR takes a dim view of organizations that are aware of the risks to patient privacy, but don’t do anything about it.

This often comes up in regard to the need for encryption, where people knew that they needed to apply encryption to systems or applications containing patient records, and then a laptop with thousands of records goes missing and it turns out there’s no encryption on the device, and perhaps no policy governing the use of mobile devices containing ePHI.

Issue #5: Lack of Transmission Security
See 45 C.F.R. §164.312(e)(2)(ii) – “When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented whenever deemed appropriate.”

Applications for which encryption should be considered when transmitting ePHI may include:

- Email (including fax by email)
- Texting
- Application sessions
- File transmissions (e.g., ftp)
- Remote backups
- Remote access and VPN sessions

It is interesting that the OCR is still seeing so many of these cases despite all the publicity around the security of email and texting in particular and the need to implement strong security policies regarding how to properly communicate ePHI with patients and other covered entities. Remember, the regulator will have the final say as to whether encryption was reasonable and appropriate, in the aftermath of a data breach.
Issue #6: Lack of Appropriate Auditing
See 45 C.F.R. §164.312(b). The HIPAA Rules require the “[implementation] of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.”

See 45 C.F.R. §164.308(a)(1)(ii)(D). Once audit mechanisms are put into place, procedures must be implemented to “regularly review records of information system activity, such as audit logs, access reports, and security incident reports.”

Activities which could warrant additional investigation:
• Access to PHI during non-business hours or during time off of by ex-employees.
• Access to an abnormally high number of records containing PHI.
• Access to PHI of persons for which media interest exists.
• Access to PHI of employees.

This is an issue that really goes to the heart of your data protection management. Had Memorial Herman been following this practice diligently, they could have saved millions of dollars!

Here is a hypothetical example that reveals the importance of a. Having an audit system in place and b. using it, regularly.

So you are viewing the logs and notice that Mary in accounting has been accessing patient files from another department. There may be a legitimate reason for that, but you also notice that she was logging in remotely, at 3am.

So maybe Mary is a hard worker, and an early riser? But a closer look at the records also reveal that she was logged in from an IP address located in Russia, and Mary lives in Ohio.

Now you realize that the person logging in at 3 am probably was not Mary, and that her account has most likely been compromised, and now you have a data breach on your hands.

So the sooner your systems can identify and stop this type of behavior, the better for all concerned.

Issue #7: Patching of Software
The use of unpatched or unsupported software on systems which access ePHI could introduce additional risk. In addition to operating systems, EMR/PM systems, and office productivity applications, software which should be monitored for patches and vendor end-of-life include:
• Router and firewall firmware
• Anti-virus and anti-malware software
• Multimedia and runtime environments (e.g., Adobe Flash, Java, etc.)

This is the first time we have seen the OCR call out this data security practice. But it is not at all surprising in light of malware such as WannaCry in which patches were available 4-6 weeks prior that would have protected companies from attack, a surprisingly high number of firms succumbed.

Those included the notorious Equifax hack, and also hundreds of healthcare providers in the British National Health System who had their operations seriously disrupted, putting patients at risk.

The fact is that most breaches are caused by failure to update software components that were known to be vulnerable for months, or even years as in the case of Equifax. So this is a very sensible recommendation.

Issue #8: Insider Threat
See 45 C.F.R. §164.308(a)(3). Organizations must “[implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information ... and to”
prevent those workforce members who do not have access ... from obtaining access to ePHI,” as part of its Workforce Security plan.

- See 45 C.F.R. §164.308(a)(3)(ii)(B). Appropriate workforce screening procedures could be included as part of an organization’s Workforce Clearance process (e.g., background and OIG LEIE checks).
- See 45 C.F.R. §164.308(a)(3)(ii)(C). Termination Procedures should be in place to ensure that access to PHI is revoked as part of a workforce exit or separation process.

More than a few data breaches involving ePHI were the result of employees accessing medical records for which they were not authorized to view. And in some cases these were celebrity patients who had their privacy violated due to curiosity or financial gain.

Unfortunately, it is not unusual for a provider to report that an ex-employee had been inappropriately accessing medical records long after they had been terminated. It is a requirement that terminated employees have their access to systems immediately terminated as well.

**Issue #9: Disposal of PHI**

See 45 C.F.R. §164.310(d)(2)(i). “When an organization disposes of electronic media which may contain ePHI, it must implement policies and procedures to ensure that proper and secure disposal processes are used.”

- The implemented disposal procedures must ensure that “electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88: Guidelines for Media Sanitization, such that the PHI cannot be retrieved.”
- Electronic media and devices identified for disposal should be disposed of in a timely manner to avoid accidental improper disposal.
- Organizations must ensure that all electronic devices and media containing PHI are disposed of securely; including non-computer devices such as copier systems and medical devices.

This can involve paper records, which on more than a few occasions have been found in dumpsters behind medical offices, and also in less obvious places such as the memory of fax machines and printers, which are just a few of the many places that PHI can hide.

**Issue #10: Backup and Contingency Planning**

See 45 C.F.R. §164.308(a)(7). Organizations must ensure that adequate contingency plans (including data backup and disaster recovery) are in place and would be effective when implemented in the event of an actual disaster or emergency situation.

- Leveraging the resources of cloud vendors may aid an organization with its contingency planning regarding certain applications or computer systems, but may not encompass all that is required for an effective contingency plan.
- See 164.308(a)(7)(ii)(D). As reasonable and appropriate, organizations must periodically test their contingency plans and revise such plans as necessary when the results of the contingency exercise identify deficiencies.

In the wake of this year’s horrendous hurricane season, this issue should be front and center. As we pointed out in a recent webinar on this subject, natural and manmade disasters can happen anywhere, any time, and usually when you least expect it.

But some things can, and should be anticipated. If you are a hospital in a flood prone coastal area, you really can’t afford to have your backup generators at ground level, or have all your servers in the basement.

Those are the kinds of issues that need to be included in a comprehensive disaster recovery plan.
WHAT ARE THE COMPLIANCE BENEFITS OF CLOUD FAX?

Your Faxes Will Be More Secure and compliant

It should be noted that HIPAA does not specify any technologies to protect ePHI. For example, 45 CFR 164.306 states:

- Ensure ePHI confidentiality
- Protect from reasonably anticipated threats
- Use any security measures that comply

That said, the OCR has embraced the encryption standards set by NIST — the National Institute of Standards and Technology. And the best cloud fax services (although not all of them) employ the strongest encryption recommended by NIST -- Transport Layer Security (TLS) version 1.2 to protect the confidentiality and integrity of data in motion.

Of course, protecting your faxes in storage is equally important in terms of both security and how well your company complies with 164.306.

For this, NIST recommends the Advanced Encryption Standard, or AES, with 256-bit encryption keys to protect data at rest.

It is true that Security Rule doesn’t expressly mandate encryption, because it is an ‘addressable’ standard. However, if your Risk Analysis and Risk Management Plans determine that encryption is a reasonable and appropriate measure to protect ePHI — it is your responsibility to implement the adequate encryption.

Another good reason is that encryption provides a safe harbor from the Breach Notification Rule. If the ePHI subject to a breach is encrypted, then “no breach notification is required following an impermissible use or disclosure of the information.”

And some healthcare organizations literally could have saved themselves millions had they only encrypted that laptop’s hard drive before it was lost.

WHAT IS THE CLOUD FAX BUSINESS MODEL?

As with most cloud-based services, you won’t need to buy, install or maintain fax machines, fax servers or any other on-premises hardware/software system to receive or send a fax. And you can disconnect those analog or digital telecom lines since all faxes, like email, will run over your existing Internet connection.

The cloud fax model moves all of the related hardware and software, management and maintenance, into the Cloud, in secure, redundant and survivable data centers. The fax service provider maintains the technology, while the end user can send and receive faxes using desktop computers, mobile devices or multi-function printers, using standard Internet access.

In this model your capital expenses for fax go to zero, as do most of the fixed recurring expenses, since you only pay for what you actually use. This frees up resources to focus on your core business mission.

### The Cloud Fax Cost Model

- **Software Costs**: Zero
- **Hardware Costs**: Zero
- **Telco Line Costs**: Zero
- **Printing Costs**: Zero
- **Maintenance Costs**: Zero
- **Power/Rackspace Costs**: Zero

### Cloud Fax Customer Costs:

1. A small monthly fee per fax number, typically includes x number of ‘free’ pages per month.
2. A fee (measured in pennies) for each fax page sent or received over the monthly allowance.

Secure cloud fax storage, if you want it, is usually included at no charge as well, although that may vary by provider and plan selected.
WHY HEALTHCARE PROVIDERS CHOOSE eFAX CORPORATE®

When it comes to enterprise-caliber cloud faxing, the world’s most widely used and widely trusted provider is eFax Corporate. Indeed, for 21 years we have been the cloud fax service of choice for more heavily regulated businesses than any other company.

To cite just two examples, one of the largest and best known healthcare providers in Cleveland, Ohio, selected eFax Corporate as their preferred fax vendor, as did the largest health insurer in a Midwestern state.

Why did these leading healthcare companies choose eFax Corporate? Because unlike most other cloud fax providers, eFax Corporate has designed our faxing technologies specifically to comply with such privacy regulations as HIPAA, GLBA, SOX, FERPA, and similar federal, state and industry regulations.

Yet another layer of security and confidence we offer our heavily regulated customers is the fact that eFax Corporate is regularly tested and certified to meet the most important security and quality assurance protocols for data protection — including ISO-27001, FIPS 140-2 and the global payment card standards body PCI-DSS.

In fact, if your organization isn’t specifically regulated by one of these federal laws or private industry regulations — or if you’re not sure whether your firm falls under the eye of any of these regulations — the security standards here might represent the most important metrics you’ll need to judge how secure is our solution.

Of course, if you know your organization falls under regulatory oversight of a data privacy law, we would be happy to give you a walkthrough of how eFax Corporate’s processes will help bring your faxing protocols into alignment with that law.

The eFax Corporate Portfolio® Check List

✓ Our solutions are trusted by many of the world’s leading businesses, in the most heavily regulated industries such as healthcare.

✓ We provide service to nearly half of the Fortune 500 companies worldwide.

✓ eFax Corporate® is certified for HIPAA compliance.

✓ Will sign a HIPAA Business Associate Agreement.

✓ Faxes in transit encrypted according to NIST recommended TLS 1.2.

✓ Faxes in storage encrypted according to NIST recommended AES 256-bit.

✓ eFax Corporate® is compliant with PCI-DSS v.3.2 encryption requirements for 2018.

✓ j2 Global® owns multiple Patents on cloud and fax technology.

✓ j2 Global® has invested millions of dollars to build a secure, compliant and redundant global cloud fax network.

✓ eFax Corporate operates on a geographically diverse global network comprised of redundant data centers and Tier III/IV rated colocations providing 99.9% server uptime.

✓ SLA for service availability and rapid Fax delivery.

✓ 24/7/365 customer support.

*Portfolio includes eFax Secure and Developer.
About eFax Corporate®
eFax Corporate is the world’s leading online fax solution, with more than 11 million customers worldwide. eFax lets users receive, review, edit, sign, send and store faxes by email or through a web interface. eFax offers plans for individual users and provides corporate solutions.

To learn more about outsourcing to a cloud fax model with eFax Corporate, visit us at:
enterprise.efax.com

©2018 j2 Global, Inc., and affiliates. All rights reserved. eFax is a brand of the j2 Cloud Connect division of j2 Global®, Inc. and a registered trademark of j2 Cloud Services™, Inc. and j2 Global Holdings Ltd.

Worldwide Headquarters
j2 Global, Inc.
6922 Hollywood Blvd.
Hollywood, CA 90028
Contact US Sales:
(888) 575-7958
Email us at:
corporatesales@mail.efax.com
Web:
enterprise.efax.com

Follow Us

Please Recycle