The 5 most common HIPAA - compliance mistakes and how to overcome them

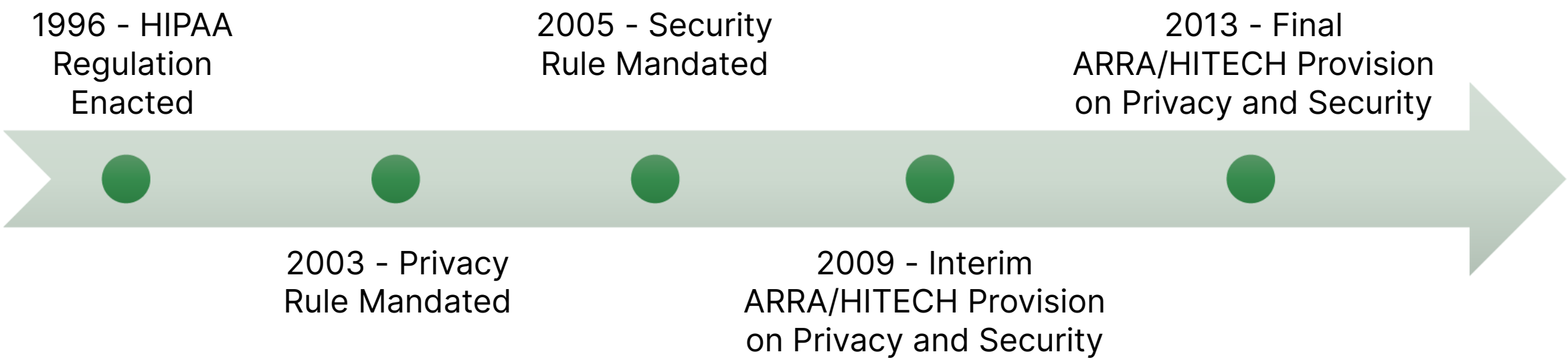
By Planet HIPAA and Jotform

Today’s Objectives

- Understand key requirements of HIPAA requirements
- Discuss Why HIPAA can’t be ignored in 2019
- Discuss common HIPAA Mistakes in 2018
- Understand simple steps to overcome common HIPAA mistakes

Health Insurance Portability and Accountability Act (HIPAA) of 1996

First attempt at development of federal rules and regulations to protect the privacy and security of Protected Health Information (PHI)



HHS, OCR Seek Industry Feedback on HIPAA Update for Data Sharing

HHS and OCR released an RFI in response to industry stakeholder requests asking Congress and HHS to modernize HIPAA for the digital healthcare age.

By Jessica Davis

December 12, 2018 - The Department of Health and Human Service and the Office for Civil Rights are seeking industry **feedback** on how to improve HIPAA guidance, especially around care coordination.

The OCR Request for Information comes in response to an outpouring of industry stakeholder requests in recent years, for a HIPAA update that reflects the digital nature of the healthcare sector.

In fact, American Medical Informatics Association and American Health Information Management Association leaders **told Congress** on December 5 that the privacy rule needed to be modernized to bolster a patient's right to access their data.

What is HHS Looking at?

In addition to requesting broad input on the HIPAA Rules, the RFI also seeks comments on specific areas of the HIPAA Privacy Rule, including:

- Encouraging information-sharing for treatment and care coordination
- Facilitating parental involvement in care
- Addressing the opioid crisis and serious mental illness
- Accounting for disclosures of PHI for treatment, payment, and health care operations as required by the HITECH Act
- Changing the current requirement for certain providers to make a good faith effort to obtain an acknowledgment of receipt of the Notice of Privacy Practices

Tell Me!

Today...

How Confident are you in your organization's HIPAA Compliance?

Tell Me!

What are your biggest barriers to feeling confident about your HIPAA Compliance Program

The Truth Is……

HIPAA Expectations...

Have created confusion and misunderstanding across organizations

Let's Talk...

Common Confusion and Misunderstanding with *HIPAA*

My organization is compliant because we have our Notice of Privacy Practices created and provide it to patients

We created policies and procedures in 2003 and 2005 and don’t need to do anything else

My organization has great practices when it comes to HIPAA and we don’t have to write them down

My organization is too small to have to implement all the HIPAA documentation requirements

My Electronic Record Vendor Took Care of Everything I Need to Do with Privacy and Security

I purchased a HIPAA Compliance Manual and it is all I need to have a compliant HIPAA program!

We educated our workforce on HIPAA previously and don’t need to do it again!

HIPAA in the EVERY News

Roper St. Francis, Valley Professionals Phishing Attacks Breach Patient Data

HealthITSecurity on Feb 3, 2019

"Charleston, South Carolina-based Roper St. Francis Healthcare and Valley Professionals Community Health Center (VPCHC) in Indiana recently began notifying patients that their data was potentially breached after employees fell victim to targeted phishing campaigns. Thirteen Roper St. Francis employees fell victim to a large-scale phishing campaign, which was discovered on November 30. Access was blocked upon discovery. Officials said the investigation determined the hacker had access between November 15 and December 15.

23,500 Patients Impacted by Connecticut Eye Clinic Ransomware Attack

HIPAA Journal on February 5, 2019

"Dr. DeLuca Dr. Marciano & Associates, P.C., a primary eye care clinic in Prospect, CT, has experienced a ransomware attack that has resulted in the encryption of files containing patients' protected health information.
The attack occurred on November 29, 2018. Prompt action was taken to shut down the network to prevent the spread of the infection, but it was not possible to stop the encryption of files on two servers used to store patient-related files. A ransom demand was received but no payment was made.
The encrypted files were successfully restored from backups.
An investigation of the breach revealed that the two servers affected by the attack contained patient files that included information such as patient names, Social Security numbers, and some treatment information.."

Improper Binder Disposal Creates PHI Privacy Concern

HealthITSecurity on December 21, 2017

"A binder containing a log with certain patient PHI was mistakenly recycled on October 17, 2017, according to an NYU Langone Health statement.
Information related to presurgical insurance authorizations from NYU Langone Health Pediatric Surgery Associates was included in the binder.
The organization's cleaning company reportedly recycled the binder, which contained certain data on approximately 2,000 patients. The information included names, dates of birth, dates of service, diagnosis codes, current procedural terminology codes, insurers' names and identification numbers.

29K Impacted by SSM Health Data Breach from Unauthorized Access

HealthITSecurity on January 4, 2018

"SSM Health recently reported that it experienced a potential data breach after an employee accessed patient records without authorization.
The access occurred between February 13, 2017 and October 20, 2017 when the employee was working in the customer service call center, according to SSM Health. At the time, the employee had PHI access to perform regular job functions."

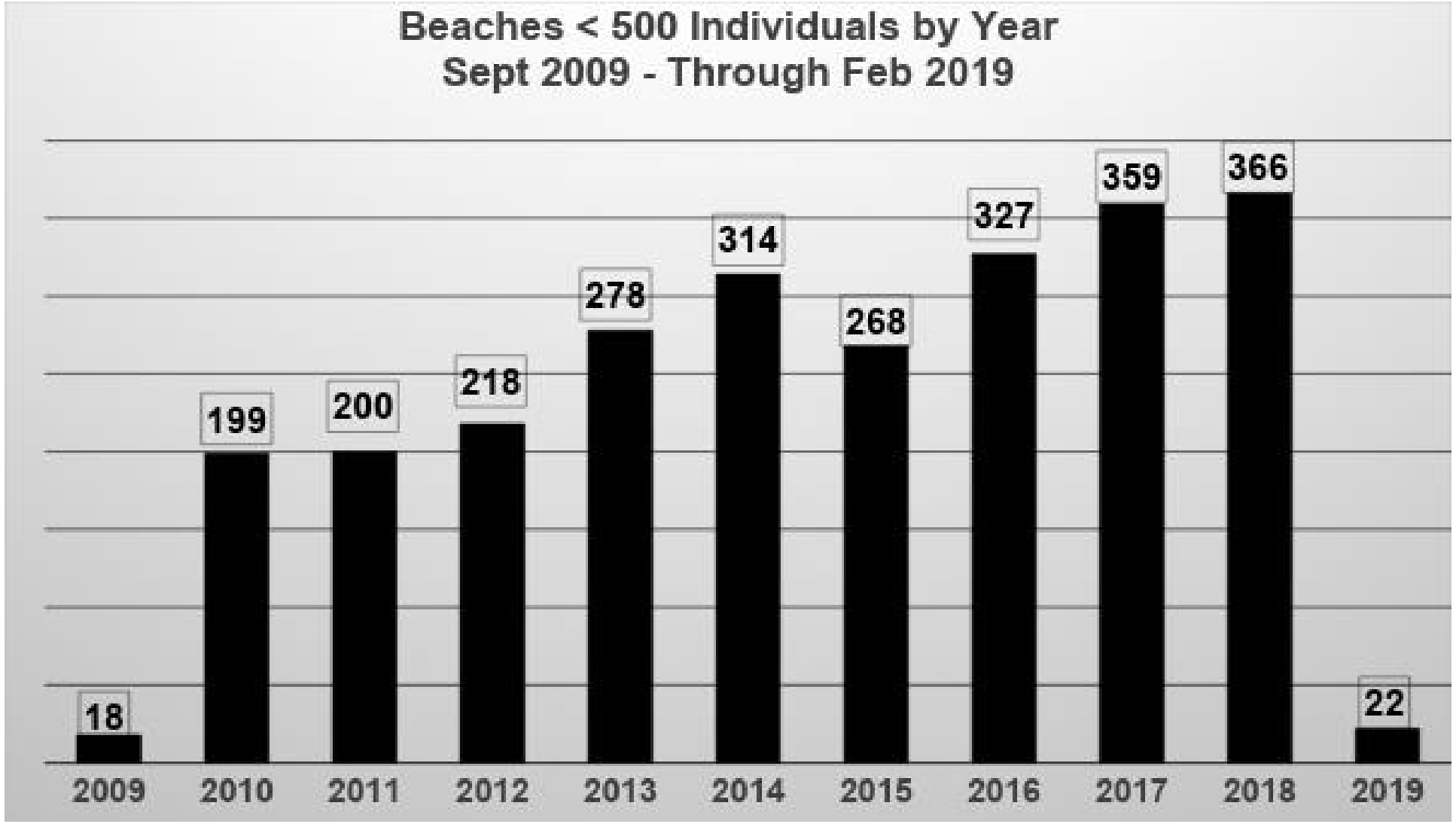
Data Breach Update

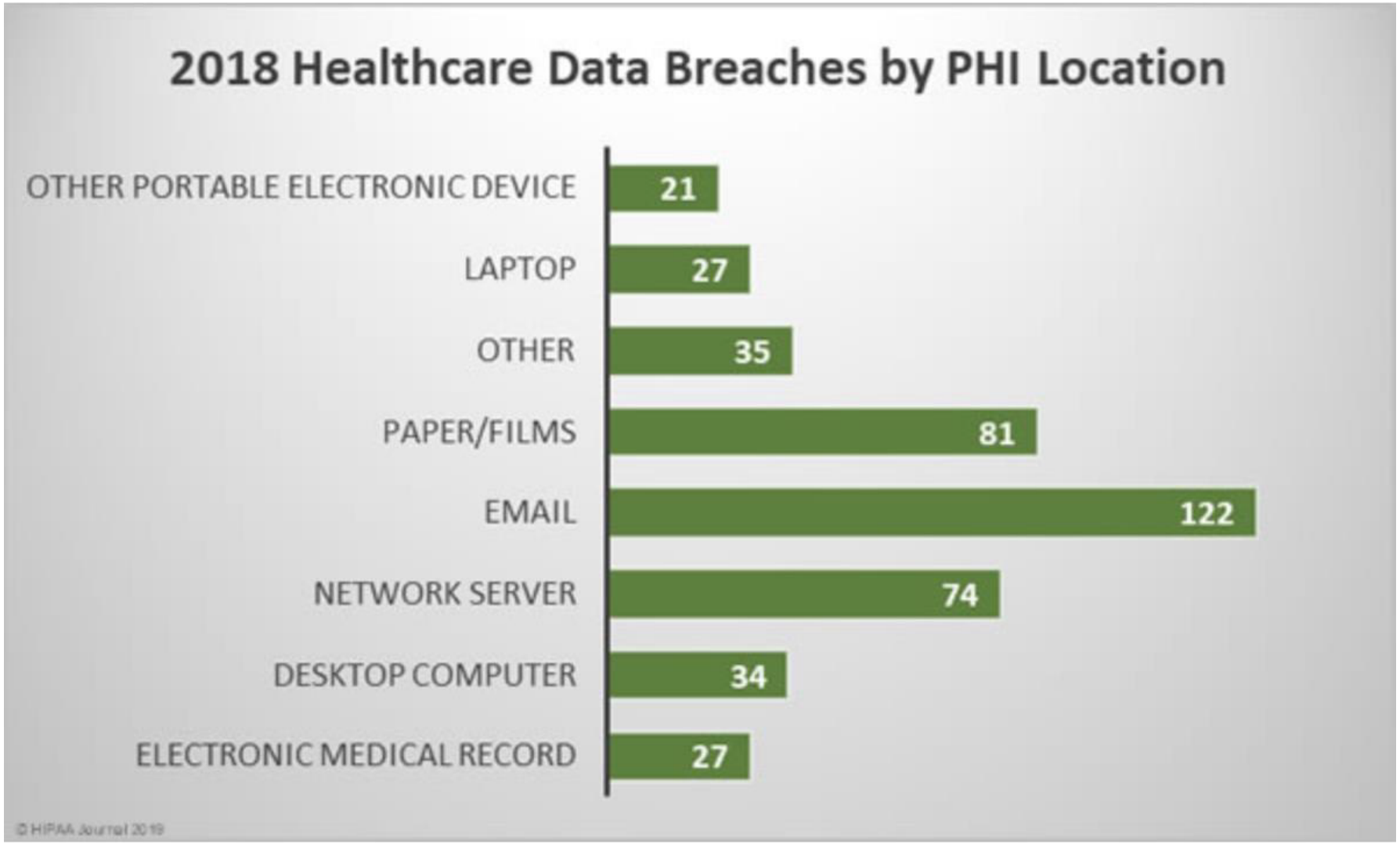
- Data Breaches continue to rise at an alarming rate
- Cybersecurity has created more threats to healthcare organizations
- 2569 Large Scale Data Breaches since September 2009
- 167,551,371 Individuals Impacted

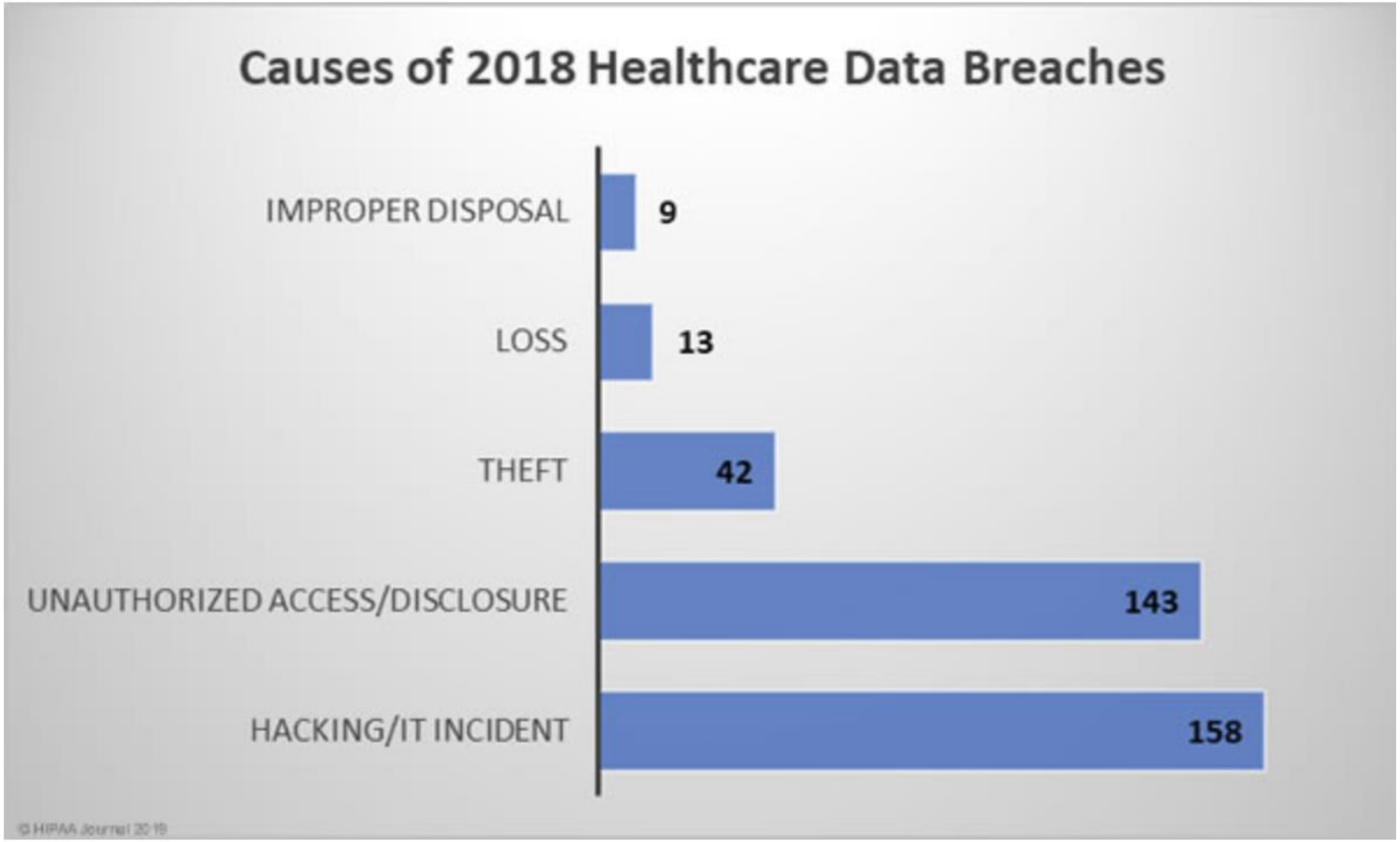
2019 (so far) – 22

- 2013 – 274
- 2018 – 366
- 2012 – 208
- 2017 -359
- 2011 – 196
- 2016 – 327
- 2010 – 198
- 2015 – 269
- 2009 – 18
- 2014 – 295\

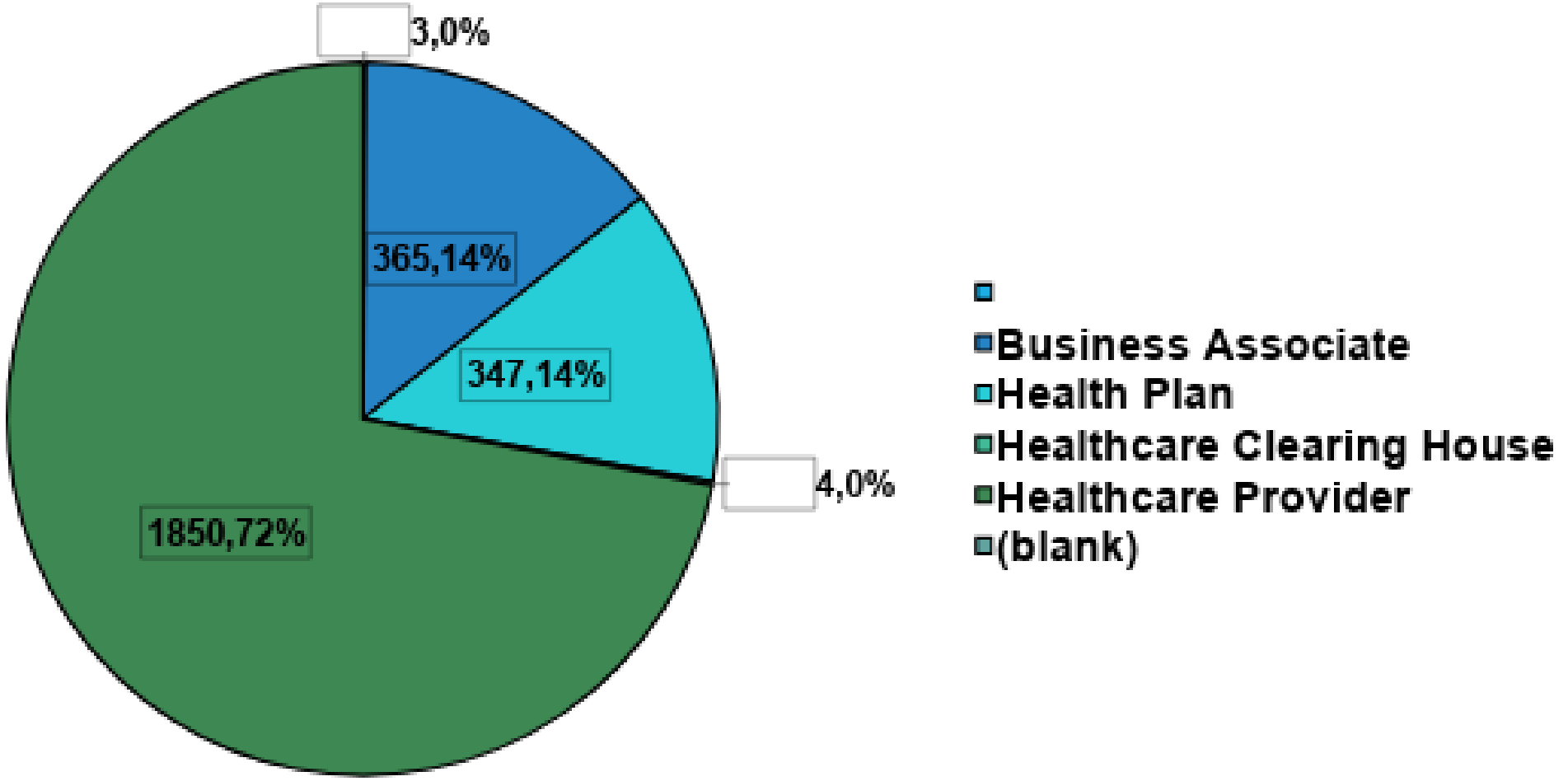
- Theft & Loss are still the leading causes of healthcare data breaches


Beaches < 500 Individuals by Year
Sept 2009 - Through Feb 2019
18
199
200
218
278
314
268
327
359
366
22
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019


2018 Healthcare Data Breaches by PHI Location
OTHER PORTABLE ELECTRONIC DEVICE
21
LAPTOP
27
OTHER
35
PAPER/FILMS
81
EMAIL
122
NETWORK SERVER
74
DESKTOP COMPUTER
34
ELECTRONIC MEDICAL RECORD
27
© HIPAA Journal 2019


Causes of 2018 Healthcare Data Breaches
IMPROPER DISPOSAL
9
LOSS
13
THEFT
42
UNAUTHORIZED ACCESS/DISCLOSURE
143
HACKING/IT INCIDENT
158
© HIPAA Journal 2019

Data Breaches < 500 Individual
By Entity Type
Sep 2009 - Feb 2019



The 5 Most Common HIPAA-Compliance Mistakes

Mistake #1:
Missing Organization Specific Policies and Procedures

HIPAA... Without a Solid Foundation

HIPAA's Policy and Procedure Requirements

- **Privacy Rule Documentation Requirement** – A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule Requirements

- **Security Rule Documentation Requirement** – Maintain the policies and procedures implemented to comply with the regulations in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment

- **Breach Notification Rule Documentation Requirement** – A covered entity is required to comply with the administrative requirements of the HIPAA Privacy Rule

How to be specifically Vague...

Sample Statement from P&Ps

"A risk analysis will be conducted in June and December every year. The risk analysis report will be provided to the Organization's Board of Directors within 10 days of the conclusion of the Risk Analysis."

Specifically Vague...

"A risk analysis will be conducted annually, with major technology changes, or updates to regulations. The risk analysis report will be provided to the Organization's Board of Directors at the conclusion of the Risk Analysis Report Generation."

Allergy practice pays $125,000 to settle doctor's disclosure of patient information to a reporter

Allergy Associates of Hartford, P.C. (Allergy Associates), has agreed to pay $125,000 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and to adopt a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Allergy Associates is a health care practice that specializes in treating individuals with allergies, and is comprised of three doctors at four locations across Connecticut.

In February 2015, a patient of Allergy Associates contacted a local television station to speak about a dispute that had occurred between the patient and an Allergy Associates' doctor. The reporter subsequently contacted the doctor for comment and the doctor impermissibly disclosed the patient's protected health information to the reporter.

OCR's investigation found that the doctor's discussion with the reporter demonstrated a reckless disregard for the patient's privacy rights and that the disclosure occurred after the doctor was instructed by Allergy Associates' Privacy Officer to either not respond to the media or respond with "no comment." Additionally, OCR's investigation revealed that Allergy Associates failed to take any disciplinary action against the doctor or take any corrective action following the impermissible disclosure to the media.

"When a patient complains about a medical practice, doctors cannot respond by disclosing private patient information to the media," said OCR Director Roger Severino. "Because egregious disclosures can lead to substantial penalties, covered entities need to pay close attention to HIPAA's privacy rules, especially when responding to press inquiries."

Allergy practice pays $125,000 to settle doctor's disclosure of patient information to a reporter

V. **Corrective Action Obligations**

Allergy Associates agrees to the following:

A. Policies and Procedures

1. Allergy Associates shall develop, maintain, and revise, as necessary, its written policies and procedures to comply with the Federal standards that govern the privacy of individually identifiable health information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the "Privacy Rule"). Allergy Associates' policies and procedures shall address, but not be limited to, the Covered Conduct specified in paragraph I.2 of the Agreement.

2. Allergy Associates shall provide such policies and procedures, consistent with paragraph 1 above, to HHS within sixty (60) days of the Effective Date for review and approval. Upon receiving any recommended changes to such policies and procedures from HHS, Allergy Associates shall have thirty (30) days to revise such policies and procedures accordingly and provide the revised policies and procedures to HHS for review and approval.

3. Allergy Associates shall implement such policies and procedures within thirty (30) days of receipt of HHS' approval.

B. Distribution and Updating of Policies and Procedures

1. Allergy Associates shall distribute the policies and procedures identified in section V.A. to all members of the workforce within thirty (30) days of HHS approval of such policies and to new members of the workforce within thirty (30) days of their beginning of service.

2. Allergy Associates shall require, at the time of distribution of such policies and procedures, a signed written or electronic initial compliance certification from all members of the workforce stating that the workforce members have read, understand, and shall abide by such policies and procedures.

3. Allergy Associates shall assess, update, and revise, as necessary, the policies and procedures at least annually or as needed. Covered Entity shall provide such revised policies and procedures to HHS for review and approval. Within thirty (30) days of the effective date of any approved substantive revisions, Covered Entity shall distribute such revised policies and procedures to all members of its workforce and shall require new compliance certifications.

Mistake #2:
Not having a Regular Process for Conducting a Risk Analysis & Mitigation Of Identified Risks

Over 95% of all HIPAA Corrective Action Plan indicate that there is a missing or insufficient Risk Analysis

HIPAA Risk Analysis

- Conduct an accurate and thorough assessment of the potential risks and vulnerability to the confidentiality,integrity, and availability of ePHI held by the covered entity
- Purpose of the Risk Analysis
    - Identify potential risks to the organization
    - Mitigate threats and vulnerabilities
    - Reduce and/or prevent potential breaches of ePHI

HIPAA Risk Management

- Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level
- Basic Steps to Risk Management
    - Plan Development
    - Implementation
    - Evaluation and Monitoring

Sample Risk Analysis Steps

1. Identify the scope of the analysis (Understand Systems with Protected Health Information).

2. Identify and document potential threats and vulnerabilities.

3. Assess current security measures.

4. Determine the likelihood of threat occurrence.

5. Determine the potential impact of threat occurrence.

6. Determine the level of risk (Likelihood + Impact = Risk).

7. Identify security measures and finalize documentation.

Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules

Fresenius Medical Care North America (FMCNA) has agreed to pay $3.5 million to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), and to adopt a comprehensive corrective action plan, in order to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. FMCNA is a provider of products and services for people with chronic kidney failure with over 60,000 employees that serves over 170,000 patients. FMCNA's network is comprised of dialysis facilities, outpatient cardiac and vascular labs, and urgent care centers, as well as hospitalist and post-acute providers.

On January 21, 2013, FMCNA filed five separate breach reports for separate incidents occurring between February 23, 2012 and July 18, 2012 implicating the electronic protected health information (ePHI) of five separate FMCNA owned covered entities (FMCNA covered entities).

The five locations of the breaches were Bio-Medical Applications of Florida, Inc. d/b/a Fresenius Medical Care Duval Facility in Jacksonville, Florida (FMC Duval Facility); Bio-Medical Applications of Alabama, Inc. d/b/a Fresenius Medical Care Magnolia Grove in Semmes, Alabama (FMC Magnolia Grove Facility); Renal Dimensions, LLC d/b/a Fresenius Medical Care Ak-Chin in Maricopa, Arizona (FMC Ak-Chin Facility); Fresenius Vascular Care Augusta, LLC (FVC Augusta); and WSKC Dialysis Services, Inc. d/b/a Fresenius Medical Care Blue Island Dialysis (FMC Blue Island Facility).

OCR's investigation revealed FMCNA covered entities failed to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of its ePHI.

Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules

A. Conduct Risk Analysis

1. The FMCNA Covered Entities shall conduct an accurate and thorough assessment of the potential security risks and vulnerabilities to the confidentiality, integrity, and availability of the FMCNA Covered Entities' electronic protected health information ("ePHI") ("Risk Analysis"). The Risk Analysis shall incorporate the FMCNA Covered Entities' facilities, whether owned or rented, and evaluate the risks to the ePHI on their electronic equipment, data systems, and applications controlled, administered or owned by the FMCNA Covered Entities, that contain, store, transmit, or receive ePHI. Prior to conducting the Risk Analysis, the FMCNA Covered Entities shall develop a complete inventory of all of their facilities, categories of electronic equipment, data systems, and applications that contain or store ePHI, which will then be incorporated into their Risk Analysis.

2. Within fourteen (14) days of the Effective Date, the FMCNA Covered Entities shall submit to HHS the scope and methodology by which they propose to conduct the Risk Analysis described in paragraph V.A.1. HHS shall notify the FMCNA Covered Entities whether the proposed scope and methodology is or is not consistent with 45 C.F.R. § 164.308 (a)(1)(ii)(A).

3. The FMCNA Covered Entities shall provide the Risk Analysis, consistent with paragraph V.A.1, to HHS within one hundred eighty (180) days of HHS' approval of the FMCNA Covered Entities' methodology described in paragraph V.A.2 for HHS' review. Within ninety (90) days of its receipt of the FMCNA Covered Entities' Risk Analysis, HHS will inform FMCNA Contact in writing as to whether HHS approves of the Risk Analysis or, if necessary to ensure compliance with 45 C.F.R. § 164.308(a)(1)(ii)(A), requires revisions to the Risk Analysis. If HHS requires revisions to the Risk Analysis, HHS shall provide FMCNA Contact with a detailed, written explanation of such required revisions and with comments and recommendations in order for the FMCNA Covered Entities to be able to prepare a revised Risk Analysis. Upon receiving notice of required revisions to the Risk Analysis from HHS and a description of any required changes to the Risk Analysis, the FMCNA Covered Entities shall have sixty (60) days in which to revise their Risk Analysis accordingly and submit the revised Risk Analysis to HHS for review and approval. This submission and review process shall continue until HHS approves the Risk Analysis.

Mistake #3:
Lack of Employee HIPAA Education

Employees and human error often top the list as the healthcare sector's biggest threat.

78% of Healthcare Workers Lack Data Privacy, Security Preparedness

Employee training programs are potentially lacking, with research showing healthcare workers do not have strong data privacy and security preparedness.

HIPAA's Policy and Procedure Requirements

- **Privacy Rule Documentation Requirement –** A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by the privacy rule and as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

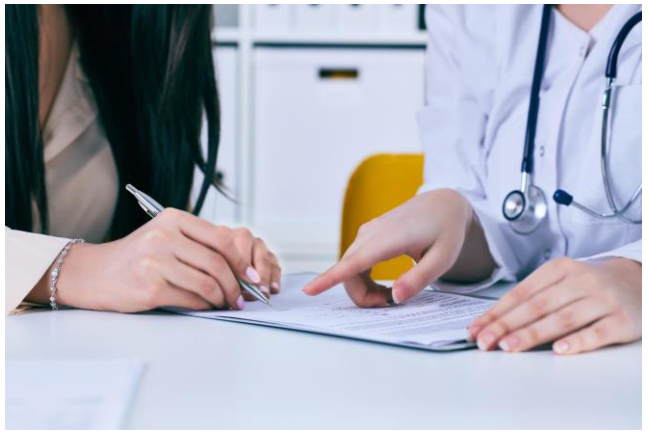
- **Security Rule Documentation Requirement –** Implement a security awareness and training program for all members of the workforce (even management)

    - Periodic Updates (A) -provide periodic security updates

- **Breach Notification Rule Documentation Requirement –** A covered entity must train all workforce members on the breach notification policy and procedures

Building a Strong HIPAA Training Program

- Establish a schedule
- Stay consistent
- Provide annual “big” HIPAA Training
- Test the Knowledge
- Provide Periodic Update
- Create a written policy and procedure
- Have an easy process for questions from workforce
- Maintain documentation



Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k

St. Luke's-Roosevelt Hospital Center Inc. (St. Luke's) has paid the U.S. Department of Health and Human Services (HHS) $387,200 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and agreed to implement a comprehensive corrective action plan. St. Luke's operates the Institute for Advanced Medicine, formerly Spencer Cox Center for Health (the Spencer Cox Center), which provides comprehensive health services to persons living with HIV or AIDS and other chronic diseases. St. Luke's is 1 of 7 hospitals that comprise the Mount Sinai Health System (MSHS).

In September 2014, the HHS Office for Civil Rights (OCR) received a complaint alleging that a staff member from the Spencer Cox Center impermissibly disclosed the complainant's protected health information (PHI) to the complainant's employer. This impermissible disclosure included sensitive information concerning HIV status, medical care, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis, and physical abuse. OCR's subsequent investigation revealed that staff at the Spencer Cox Center impermissibly faxed the patient's PHI to his employer rather than sending it to the requested personal post office box. Additionally, OCR discovered that the Spencer Cox Center was responsible for a related breach of sensitive information that occurred nine months prior to the aforementioned incident but had not addressed the vulnerabilities in their compliance program to prevent impermissible disclosures.

"Individuals cannot trust in a health care system that does not appropriately safeguard their most sensitive PHI," said Roger Severino, OCR director. "Covered entities and business associates have the responsibility under HIPAA to both identify and actually implement these safeguards. In exercising its enforcement authority, OCR takes into consideration aggravating factors such as the nature and extent of the harm caused by failure to comply with HIPAA requirements."

Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k

C. Training

1. St. Luke's shall review and revise, as necessary, its current training materials to include instructions on safeguarding PHI when providing individuals such information, which shall include instructions on providing individuals with such information by mail, fax, or other electronic transmission. St. Luke's shall provide HHS with the training materials for all workforce members within thirty (30) calendar days of the Effective Date. HHS shall provide any comments on or approve the training materials within sixty (60) calendar days of receipt.

2. Upon receiving notice from HHS specifying any required changes, St. Luke's shall make the required changes and provide revised training materials to HHS within thirty (30) calendar days. HHS shall provide any further comments on or approve the revised materials within thirty (30) calendar days of receipt. This process shall continue until HHS approves the training materials.

3. Upon receiving approval from HHS, St. Luke's shall provide training using the approved training materials for all workforce members within the later of sixty (60) calendar days of HHS' approval or by October 31, 2017. St. Luke's shall also provide training using the approved training materials at least every twelve (12) months thereafter. St. Luke's shall also provide such training to each workforce member that is responsible for faxing and transmitting PHI within thirty (30) calendar days of the commencement of such workforce member's service.

4. Each workforce member who is required to attend training shall certify, in electronic or written form, that he or she has received the training. The training certification shall specify the date training was received. All course materials shall be retained in compliance with Section VII.

5. St. Luke's shall review the training at least annually, and, where appropriate, update the training to reflect changes in Federal law or HHS guidance, any issues discovered during audits or reviews, and any other relevant developments.

6. St. Luke's shall not provide access to PHI to any member of its workforce if that workforce member has not signed or provided the written or electronic certification required by Paragraph V.B.2 of this section within three (3) months of distribution of such policies and procedures to the members of its workforce, but in any event no later than January 31, 2018.

Mistake #4:
Not Establishing Business Associate Agreements

What is a Business Associate?

- A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

- An individual or organization that creates, receives, maintains, or transmits protected health information on behalf of a covered entity

- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity, if the service involves the disclosure of PHI.

- Mere Conduits – narrow definition and only apply to courier services such as the Postal Service or Internet Service Provider

Requirements of a Business Associate Agreement

- Describe the permitted and required uses of protected health information by the business associate
- Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law
- Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.
- Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement.
- If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

No Business Associate Agreement? $31K Mistake – April 20, 2017

The Center for Children's Digestive Health (CCDH) has paid the U.S. Department of Health and Human Services (HHS) $31,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and agreed to implement a corrective action plan. CCDH is a small, for-profit health care provider with a pediatric subspecialty practice that operates its practice in seven clinic locations in Illinois.

In August 2015, the HHS Office for Civil Rights (OCR) initiated a compliance review of the Center for Children's Digestive Health (CCDH) following an initiation of an investigation of a business associate, FileFax, Inc., which stored records containing protected health information (PHI) for CCDH. While CCDH began disclosing PHI to Filefax in 2003, neither party could produce a signed Business Associate Agreement (BAA) prior to Oct. 12, 2015.

Florida contractor physicians' group shares protected health information with unknown vendor without a business associate agreement

Advanced Care Hospitalists PL (ACH) has agreed to pay $500,000 to the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) and to adopt a substantial corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. ACH provides contracted internal medicine physicians to hospitals and nursing homes in west central Florida. ACH provided services to more than 20,000 patients annually and employed between 39 and 46 individuals during the relevant timeframe.

Between November 2011 and June 2012, ACH engaged the services of an individual that represented himself to be a representative of a Florida-based company named Doctor's First Choice Billings, Inc. (First Choice). The individual provided medical billing services to ACH using First Choice's name and website, but allegedly without any knowledge or permission of First Choice's owner.

On February 11, 2014, a local hospital notified ACH that patient information was viewable on the First Choice website, including name, date of birth and social security number. In response, ACH was able to identify at least 400 affected individuals and asked First Choice to remove the protected health information from its website. ACH filed a breach notification report with OCR on April 11, 2014, stating that 400 individuals were affected; however, after further investigation, ACH filed a supplemental breach report stating that an additional 8,855 patients could have been affected.

$1.55 million settlement underscores the importance of executing HIPAA business associate agreements

North Memorial Health Care has agreed to settle charges that it potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to implement a business associate agreement with a major contractor and failing to institute an organization-wide risk analysis to address risks and vulnerabilities to its patient information. North Memorial is a comprehensive, not-for-profit health care system in Minnesota that serves the Twin Cities and surrounding communities. The settlement includes a monetary payment of $1,550,000 and a robust corrective action plan.

$750,000 settlement highlights the need for HIPAA business associate agreements

Raleigh Orthopaedic Clinic, P.A. of North Carolina (Raleigh Orthopaedic) has agreed to pay $750,000 to settle charges that it potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule by handing over protected health information (PHI) for approximately 17,300 patients to a potential business partner without first executing a business associate agreement. HIPAA covered entities cannot disclose PHI to unauthorized persons, and the lack of a business associate agreement left this sensitive health information without safeguards and vulnerable to misuse or improper disclosure. Raleigh Orthopaedic is a provider group practice that operates clinics and an orthopaedic surgery center in the Raleigh, North Carolina area.

OCR initiated its investigation of Raleigh Orthopaedic following receipt of a breach report on April 30, 2013. OCR's investigation indicated that Raleigh Orthopaedic released the x-ray films and related protected health information of 17,300 patients to an entity that promised to transfer the images to electronic media in exchange for harvesting the silver from the x-ray films. Raleigh Orthopedic failed to execute a business associate agreement with this entity prior to turning over the x-rays (and PHI).

Mistake #5:
Lack of Use of
Technical Safeguards

HIPAA is a ‘Technology Neutral’ Regulation

HIPAA is scalable and allows for flexibility

Interpretation is not to use technology to support compliance

Addressable v. Required

- Standards are broken up into two categories (45 CRF 164.306(d))
- **Addressable** – the covered entity must assess the reasonableness and appropriateness of the safeguard to protect the entity's ePHI
  - The size, complexity and capability of the covered entity
  - The covered entity technical infrastructure, hardware, and software security capabilities
  - The costs of security measures
  - The probability and criticality of potential risks to ePHI.
- **Required** – the covered entity must comply with the standard and implement policies and/or procedures that meet the requirement

Examples How Technology Can Support Compliance

- Encryption for Data at Rest (computers, server)
- Encryption for Data in Motion (e-mail)
- Notification of Inactive Users
- Usernames and Passwords
- Intrusion Detection Software
- Update to Date Antivirus Solution
- Strong Firewall
- Backup Solutions

Is JotForm HIPAA Compliant?

Posted By HIPAA Journal on Mar 5, 2019

HIPAA Compliant Forms on Websites

HIPAA covered entities can use online forms to collect a wide range of information from patients. Online forms are useful for registering new patients, obtaining consent, conducting customer surveys, and taking payments. Web forms streamline data collection, allow patient information to be sent to EHRs or other internal systems quickly and efficiently, and they can improve the patient experience.

HIPAA covered entities that have the resources can create online forms manually; however, those that lack staff with the necessary skills or have to create large numbers of forms will benefit from using online form software to speed up the process of creating online forms.

Is JotForm HIPAA Compliant?

JotForm is one of the most popular online form software providers with over 4 million users worldwide, but can the software be used by healthcare providers for creating HIPAA compliant forms?

JotForm protects customer data through a 256 Bit SSL connection and RSA 2048 encryption is used for data storage and transmission. The software also features access controls to limit who can view form data.

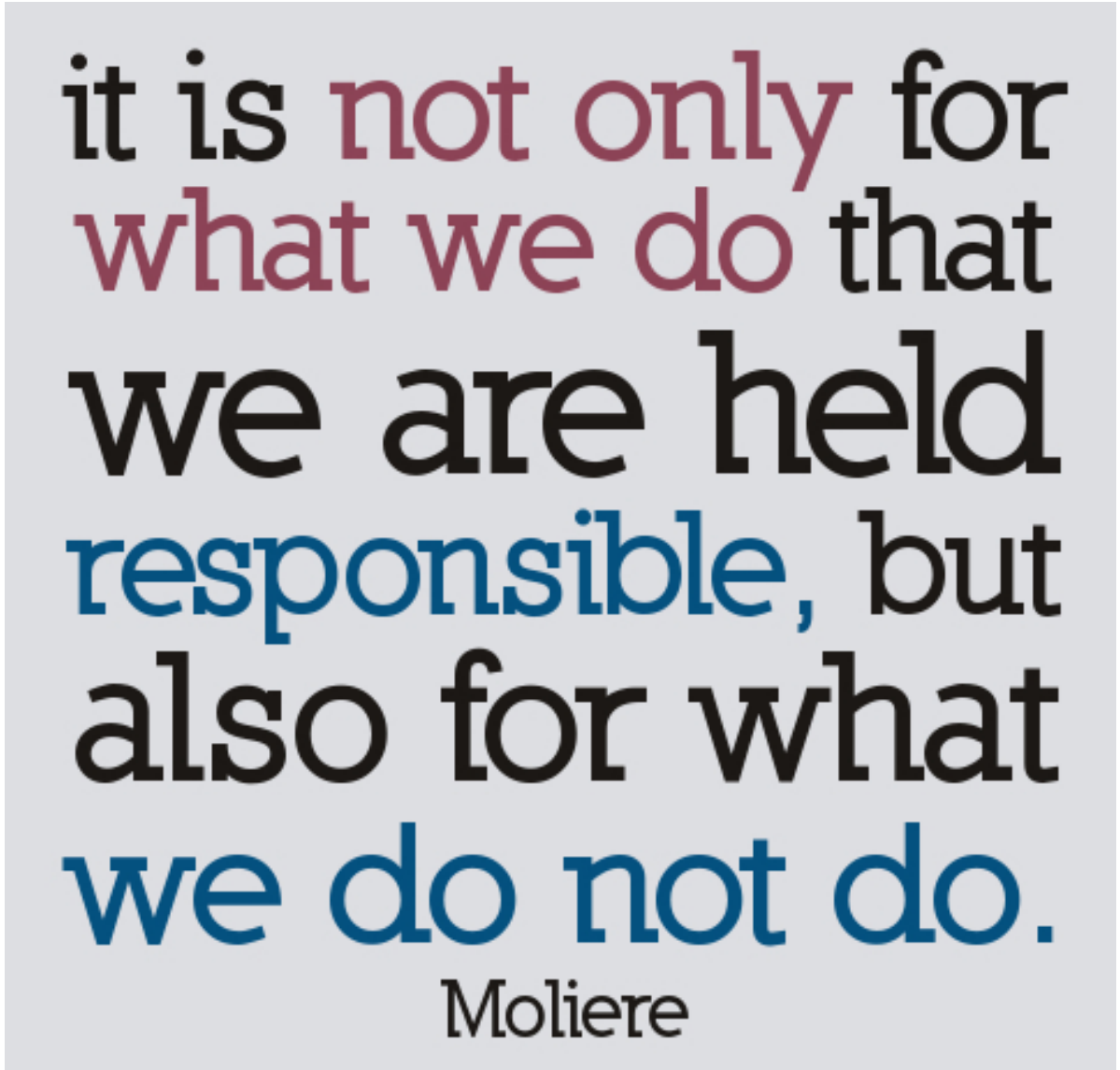
Importantly, in addition to providing a secure online form solution, JotForm is prepared to enter into a BAA with HIPAA covered entities that sign up for JotForm. As long as healthcare organizations obtain a BAA from JotForm, it is a a HIPAA compliant online form solution for healthcare organizations and can be used in connection with ePHI.

ENCRYPTION

Unsure of how you are doing
With HIPAA Compliance

Try Out our Free HIPAA Check Up

https://www.planethipaa.com/hipaa-checkup


it is not only for
what we do that
we are held
responsible, but
also for what
we do not do.
Moliere

References

- https://healthitsecurity.com/news/reduce-employee-email-risk-by-takingdecisions-away-from-users
- https://www.hhs.gov/hipaa/for-professionals/complianceenforcement/agreements/index.html
- www.hipaajournal.com
- https://www.jotform.com/what-is-hipaa-compliance/