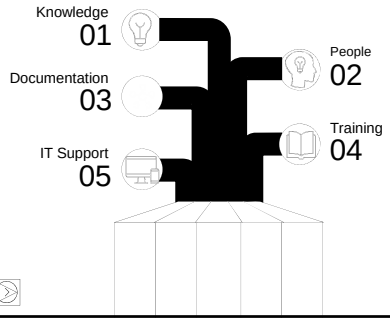
Five Must Haves to Make HIPAA Compliance Easy

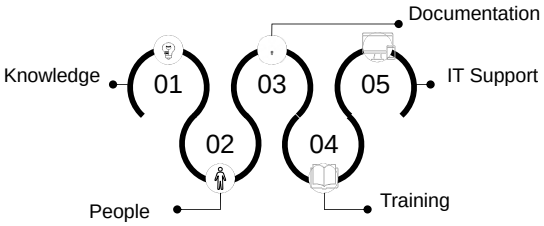


Hello!

I'm Karen Gregory. I am a compliance nerd.

- Employee of Total Medical Compliance, a Key Opinion Leader for Hu-Friedy, and on the OSAP Board of Directors.
- No commercial support has been provided for this activity. Any reference to a commercial product is for example purposes only and does not reflect endorsement

HIPAA Made Easy

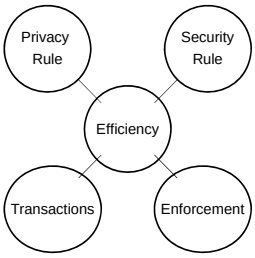


Knowledge

Knowledge is of no value unless you put it into practice – Anton Chekhov

One P Two As

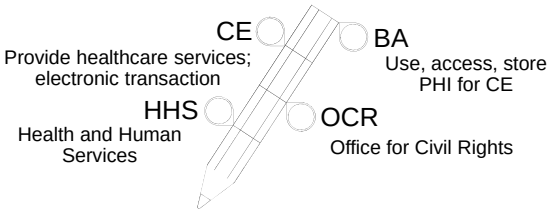
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT



- Transactions - Format for transmission of claims
- Privacy - Patient rights and actions to ensure privacy of information
- Security – Safety of PHI in electronic format
- Enforcement - Accountability

PHI – Protected health information

ePHI – PHI in an electronic format



All work together to protect patient information

Protected Health Information
Oral, Written, Electronic Format

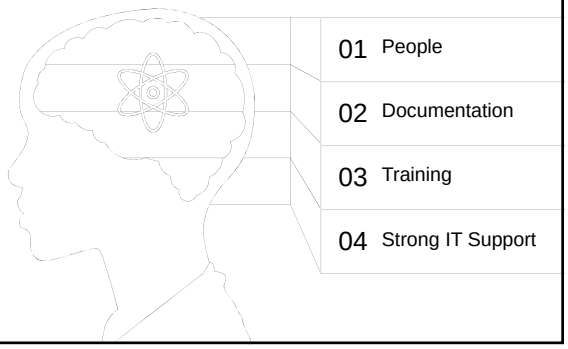
- Names
- All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code

7

American Recover and Reinvestment Act
Putting Your Tax Dollars to Work

8

Knowledge Drives the Rest



01 People
02 Documentation
03 Training
04 Strong IT Support

Workers - Use or Release of Information

- For treatment, payment and healthcare operations after providing a Notice of Privacy Practices
- To the individual or legal representative
- To friends and family with informal approval or for emergencies.
  - –Should ask the patient for permission to discuss healthcare if accompanied by another person during exam
- As authorized by the patient
- Based on professional judgment of the healthcare provider which is in the best interest of the patient

10

Notice of Privacy Practices

- Given to all new patients
- Outlines:
  - –Patient rights under the Privacy Rules
  - –Summary of the entities privacy practices
  - –Summary of current uses and disclosures of PHI and examples of each type
- Acknowledgment of Receipt maintained in patient record
- Posted in Waiting Area and prominently on website

11

Accountability Under HIPAA

- For the practice/business associates:
  - –Settlements range from $100 – $50,000 per incident, up to a total of 1.5 million for practices, business associates.
- For employees:
  - –Monetary amounts from $50,000 - $250,000 and from 1 – 10 years in prison.
  - –If offense is committed with *intent to sell, transfer, or use* individually identifiable health information *for commercial advantage, personal gain, or malicious harm,* be fined not more than $250,000, imprisoned not more than 10 years, or both.

12

Patients' and Their Rights

- Access - Review and obtain a copy of their PHI
- Amendment - Request covered entities amend their PHI
- Disclosure Accounting –Where or with who PHI is shared
- Restriction Request –
  - –Disclosure to persons involved in the individual's healthcare
  - –Disclosure to notify family members or others about the individual's general condition, location, or death
  - –Disclosure to payers if services paid for out of pocket
- Confidential Communications – Phone, voicemail

13

Friends and Family

- Relevant information may be shared with family members or friends involved in the patient's care or payment for your health care:
  - –if the patient has provided permission, or if they do not object to sharing of the information.
- If the patient is not present or unable to give permission:
  - –health care provider may share or discuss health information with family, friends, or others involved in the care or payment of care if the provider believes that it is in the patient's best interest
- Information should not be shared which is not pertinent to the involvement/situation

14

Access Request

- An access request is driven by the patient and may include a request to send information to a third party
  - –Required with a few exceptions to comply with the request
  - –Specified times on when the information must be provided
- Convenient time and place to pick up the copy or inspect the PHI
  - –Mail or fax
  - –Patient portal
  - –Flash drive/CD
  - –Email
  - –Written summary

15

Request for electronic copies

- *PHI stored electronically* – Must provide the information in the requested electronic form and format, if it is readily producible
  - –Must be able to provide at least one type of readable, electronic format
- It information cannot be provided in the requested format (example, a Word document)
  - –Work with the individual to find an acceptable alternative
  - –If all electronic options are declined, then provide a paper copy

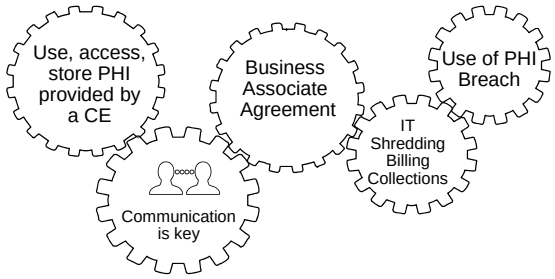
16

Fees

- Reasonable and cost-based
- May cover the following costs:
  - –labor for copying the PHI
  - –supplies for creating the copies
  - –postage, if mail is requested
  - –summary preparation, if requested
- Fees must not include costs associated with verification, and documentation search and retrieval even if allowed by State law

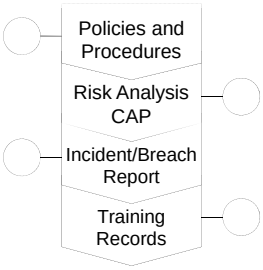
17

Business Associates

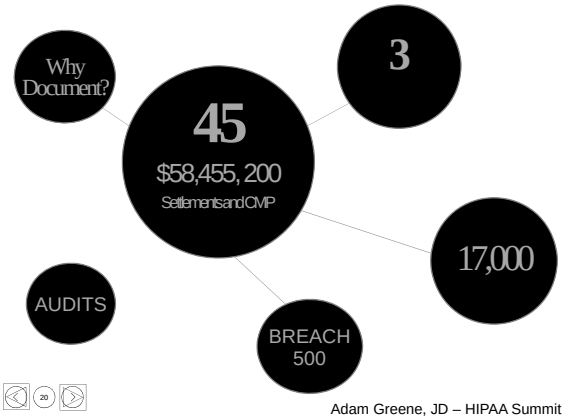


18

Documentation



19



20

Adam Greene, JD – HIPAA Summit

Why Audit – Snapshot in Time

- The HITECH Act, section 13411
  - –Mandates (HHS) conduct periodic audits to assess both covered entity and business associated compliance with HIPAA Privacy and Security Rules and Breach Notification Standards.
- Opportunity to:
  - –Encourage renewed attention to compliance
  - –Examine mechanisms for compliance
  - –Identify best practices
  - –Discover risks and vulnerabilities that may not have come to light through complaints and compliance reviews

21

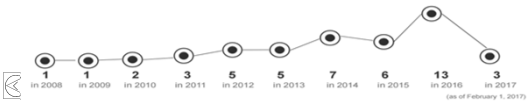
Phase 2 Audits - Desktop

- Focus - Privacy/Breach audit:
  - NPP (includes URL for electronic NPP)
  - Patient Right to Access policies
  - Review of actual Access timing and methods
  - Review of actual Breaches
  - Breach letters actual and templates
  - Breach policies and procedures
- Focus - Security Audit:
  - Risk Analysis both actual and process
  - Risk Management actual and process
- Both audits include requests for current and past (as much as six years back) documentation

22

Iliana Peters (OCR) - Enforcement

- Enforcement activity highest in 2016 – cases in the pipeline
- Very little of what this sector does – 17,000 complaints closed each year
- Focus is to provide education through enforcement activities based on egregious activities
- Entities are not taking cybersecurity seriously enough – need understanding of what is at risk
- Risk Analysis - Enterprise wide or ALL risks, not just the EHR



Polices and Procedures

- Establishes standards and sets expectations
- Just a few must haves:
  - –Sanctions policy – Each worker should know for what they will be held accountable and the discipline which will be applied
  - –Policies to address protection and release of PHI
    - Access
    - Reasonable safeguards – Sign-in sheets, visitors
    - Law enforcement – Dental records
    - Legal issues – Subpoena
  - –Employee behaviors – Use of network for personal social media, internet browsing

24

Risk Analysis - Security Rule

- **§ 164.308**
- (a) A covered entity must:
  - –(1)(i) Implement policies and procedure to prevent, detect, contain, and correct security violations.
  - –(ii) Implementation specifications:
    - (A) *Risk analysis* - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
- For a successful analysis, IT MUST be involved

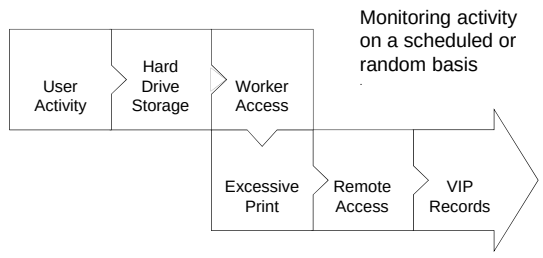
25

HHS on Risk Analysis process

- Maintain continuous, reasonable, and appropriate security protections
- Ongoing process of regular reviews of records to track access to ePHI to detect security incidents
- Evaluate the likelihood and impact of potential risks to ePHI
- Implement appropriate security measures to address the risks identified
- Document the chosen security measures and, where required, the rationale for adopting those measures

26

Risk – The Role of Audits



27

Evaluation of Past Events

RISK ANALYSIS ADDENDUM

Complete this section and store with the Risk Analysis.

Provide a brief description of Security and/or Privacy incidents in the past 12 months.

- ☐ Breach (Theft of computer, accessing patient records for curiosity, mail to an incorrect address which was opened)
- ☐ Breach exclusion (Access of patient account by worker accidentally)
- ☐ Security Incident (attempted hacking, virus)

Action Taken to Prevent or Correct Issues

1. List corrective actions implemented to prevent reoccurrences of items listed above:
   - ☐ Policy review/update

28

Corrective Action Plan

- Risk analysis process is the first step
- Documentation to address vulnerable areas must be in place
- Identification of the issue without correction is unacceptable to HHS

1. Vulnerability (Area of weakness outlined in the Risk Analysis)	2. Type of Threat Represented (Check all that Apply)	3. Likelihood weakness will impact the organization Self-Assessment	4. Level of damage if impacted Self-Assessment	5. Plan of Action Our organization will either eliminate or minimize the vulnerability (weakness) in the following ways. *Additional Documentation Attached if needed	6. Responsible Party Time Frame for Completion Initial when project complete
Lack of adequate anti-virus protection for laptops	☐ Human ☐ Natural X Technical ☐ Environmental ☐ Operational	X High ☐ Medium ☐ Low	X High ☐ Medium ☐ Low	1. Review policies on purchase of new hardware. 2. Recall current inventory. 3. Install software to protect the mobile device.	IT Department 30 days
New hire employees are not provided HIPAA training	☐ Human ☐ Natural ☐ Technical ☐ Environmental X Operational	☐ High X Medium ☐ Low	☐ High X Medium ☐ Low	1. Identify all employees who have not been trained. 2. Provide instructions on access to TMC on-line training. 3. Allow adequate time to complete training modules. 4. Workers must pass posttest with 80% score.	Manager 30 days

BREACH

- The unauthorized acquisition, access, use, or disclosure of PHI not permitted under the privacy rule, which compromises the security or privacy of such information.
- This activity is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.

30

Breach: Not if. When? How many?

Healthcare Provider	19727	04/04/2017	Hacking/IT Incident	Network Server
Healthcare Provider	685	04/03/2017	Unauthorized Access/Disclosure	Other
Business Associate	1132	03/31/2017	Hacking/IT Incident	Network Server
Healthcare Provider	55447	03/26/2017	Hacking/IT Incident	Network Server
Healthcare Provider	80270	03/25/2017	Hacking/IT Incident	Email
Health Plan	732	03/23/2017	Unauthorized Access/Disclosure	Paper/Films
Healthcare Provider	960	03/23/2017	Theft	Desktop Computer, Laptop
Healthcare Provider	279663	03/22/2017	Hacking/IT Incident	Network Server
Healthcare Provider	1298	03/20/2017	Unauthorized Access/Disclosure	Paper/Films
Healthcare Provider	967	03/20/2017	Unauthorized Access/Disclosure	Paper/Films
Health Plan	1320	03/17/2017	Unauthorized Access/Disclosure	Paper/Films

Only Allowable Breach Exclusions

- EXAMPLES
  - –Worker logs into the wrong patient's record
  - –Worker sends information to another worker in the practice who is not involved in the care of the patient
  - –As a patient is checking out, handed the visit summary of another patient.
    - The paperwork is immediately returned
    - Patient in receipt of the wrong paperwork did not have time to retain the information

32

Documentation

BREACH/ INCIDENT INVESTIGATION REPORT

Report Date _____ **Incident Date** _____

Practice Name _____

Practice Address _____

Description of the incident - Describe the incident/use/disclosure with information relevant to how it happened, how it was detected, individuals involved, how it was reported, etc.

_____

_____

_____

_____

_____

Record elements of the investigation – Reports reviewed, people talked to, etc.

_____

Breach Investigation

- All staff must understand who to notify *immediately*
- Patients must be notified without reasonable delay and no later than 60 days of the discovery
- Breaches involving 500 or more individuals: notification of the local prominent media and HHS
- Notification may be costly
  - –Action by Office for Civil Rights
  - –Reputation
  - –Legal claims/lawsuits
  - –Individual workers can be held liable

34

Breach Notification and the BA

- Provide notice to the covered entity (CE) without reasonable delay, no later than 60 days from the discovery of a breach.
- MUST address timing of reporting in the BA contract
- CE has ultimate responsibility to report the breach
  - Reporting may be delegated by contract to the BA
  - Does not lessen the responsibility of the CE
  - Both parties should NOT report

35

Patient Notification Process

- Written notice to affected individuals:
  - First class mail or by electronic mail if permission provide
  - May take MORE than one mailing to provide information
  - If urgent may call, but must be followed by written notice
- For insufficient contact information for 10 or more individual:
  - Conspicuous posting on the home page of the covered entity's Web site for 90 days
  - Notice in major print/broadcast media
  - Toll-free number for patient questions

36

Patient Notification

- Brief description of what happened
- Description of the types of unsecured PHI involved in the breach (name, Social Security Number, etc.)
- Steps individuals should take to protect themselves
  - Many entities' provide credit monitoring services.
- Brief description of what is being done to investigate the breach, mitigate damage, and protect against further breaches.
- Contact information for questions by patients.

37

Training Records

- How would you prove workers have been trained and REMINDED about safety of PHI?
- Training topics
  - Sanctions policy
  - Elements of the Privacy and Security Rules
  - Minimum necessary
  - Reasonable safeguards
  - Release of information
  - How to report a breach
  - Social Media
  - Cybersecurity

38

Strong IT Support

Accurate ePHI must be available to provide services

39

Risks to ePHI

Confidentiality 01

Availability 02

Integrity 03

04 Cyber-criminals

1. Natural disasters
2. Accidental/intentional destruction of ePHI
3. Theft – computers, servers

Dental practices are targeted for the information in the patients records

40

KNOW the Location of ePHI

- Laptops, office PCs, servers
- Smartphones
- Thumb or flash drives
- Back up devices
- CD/DVD
- Website – Appointment requests
- Equipment
  - –Fax or copiers
  - –CAD/CAM
- ePHI during transmission
  - –Email
  - –Referral dentist
  - –Patients

41

Ransomware

- Encrypts the data of the target, requires a ransom for the “key”
- HHS has issued guidance: ransomware attack is a breach
  - Uses the terminology “facts and circumstances analysis”
  - Did the criminal access the information? Now selling the data they encrypted
  - Bigger issue is denial of service which may constitute a breach
  - Data encrypted falling into safe harbor – well…. Yes and no
- Protections
  - Risk analysis
  - Appropriate back-ups and TESTING
  - Contingency planning

42

Ransomware

- Encrypts the data of the target, requires a ransom for the "key"
- HHS has issued guidance: ransomware attack is a breach
  - Uses the terminology "facts and circumstances analysis"
  - Did the criminal access the information? Now selling the data they encrypted
  - Bigger issue is denial of service which may constitute a breach
  - Data encrypted falling into safe harbor – well…. Yes and no
- Protections
  - Risk analysis
  - Appropriate back-ups and TESTING
  - Contingency planning

43

Outsider Threats

Phishing Scheme Example

- Receptionist or any other front line employee receives email from what appears to be a legitimate vendor of employer.
- May warn of compromise to user credentials or account
- Will provide link to update credentials
- Receptionist clicks on link
- Gives Cyber-criminal access

44

Safeguarding ePHI

- Strong passwords which are changed routinely
- Log off or lock computer when leaving work area
- Ensure security updates to protect against malware, viruses
- Physical security - mobile devices containing ePHI
- Only open email/attachments from reliable sources
- Access only approved internet sites
- Do not mention patients on personal social media accounts.
- Data encryption – back-up devices, phones, servers, computers.

45

Encryption - NIST

- Provided by National Institute of Standards and Technology
- Advanced Encryption Standard (AES) – 256
- Items to consider:
  - –Portable devices – Laptops, thumb/flash drives, smart phones
  - –Devices in your office – Computers in practice, copiers, scanners, fax
  - –Server – need to weigh risk
  - –Information being transmitted
  - –Media being transported
  - –Business Associate data

46

To Do

- Ensure all workers are trained on protection of patient information
  - –How are new workers trained?
  - –Is training provided that is specific to the persons job description?
  - –What about forms such as the NPP and Access and Authorization forms?
- Review all policies and procedures
  - –Is there a specific policy on breach identification, evaluation and reporting?
  - –Do workers know how to report a breach or suspected breach?
  - –Are business associate agreements in place and current?

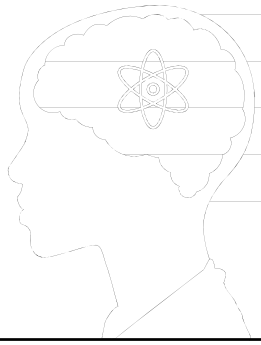
47

Be Prepared

- Know your practice – where is information stored? Does it leave the practice? Who has access? Can you answer how all PHI is protected?
- Documentation will be crucial
- A strong compliance program includes a Risk Analysis
- Develop a Contingency Plan which includes testing of backed-up data
  - –Can you restore lost data?
- Be on the look out for any communication from Office for Civil Rights
- Greater risk of an audit from a breach than from the random audit process

48

Final Thoughts



01 People

02 Documentation

03 Training

04 Strong IT Support

Final Thoughts

People – Biggest asset, biggest risk

Documentation – Keep for six years

Training - Your best protection

Strong IT – Non-negotiable

50

Thank You!

Contact Information

Karen Gregory, RN

Karen@TotalMedicalCompliance.com

51

Resources

- HIPAA for Professionals
  - https://www.hhs.gov/hipaa/for-professionals/index.html
- Security Rule Educational Paper Series
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- HHS Guidance on Patient Access
  - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
- Enforcement Information
  - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

52

Request for Access to Personal Health Information

Patient Name: _____ DOB: _____

Address: _____

City-State, Zip: _____

Home Phone: _____ Work Phone: _____

- ☐ I would like a copy of my health information – I understand I may be charged a reasonable cost based fee.
- ☐ I would like to review my health information
- ☐ I would like for my health information to be provided to a third party:
  - o Name of third party: _____

Please specify the records included in this request:

_____

_____

Select the format you would prefer:

- ☐ Paper
  - ☐ Mail to above address
  - ☐ Will pick up at the practice
- ☐ Electronically
  - ☐ Flash Drive/CD
  - ☐ Patient Portal
  - ☐ Email
- ☐ Fax Number: _____

  - o Email address: _____
  - o For **email communication,** I understand that if information is not sent in an encrypted manner there is a risk it could be accessed inappropriately. By providing my email address I elect to receive email communication as requested.

- ☐ I would like a written summary of the requested information. I understand that I may be charged a reasonable cost based fee.

You will receive notification regarding this access request no later than 30 days from the date received. There are limited circumstances in which your request may be denied, some of which you may have the right to request a review of the decision.

_____Date _____

Signature of Patient or Personal Representative

*Description of Personal Representative's Authority (attach necessary documentation)

Forward this request to Privacy Officer or Office Manager

For office use only:

Date Received: _____ By: _____

☐ Request Accepted ☐ Request denied

If denied, provide reason(s):

Reviewable grounds:

- ☐ The access is reasonably likely to endanger the life or physical safety of the individual or another person
  - This ground for denial does not extend concerns that the individual will not be able to understand the information or may be upset by it
- ☐ The access requested is reasonably likely to cause substantial harm to a person (other than a health care provider) referenced in the PHI
- ☐ The provision of access to a personal representative of the individual that requests such access is reasonably likely to cause substantial harm to the individual or another person

Unreviewable grounds:

- ☐ Request is for psychotherapy notes, or information compiled in reasonable anticipation of, or for use in, a legal proceeding
- ☐ An inmate requests a copy of their PHI and providing the copy would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other persons at the institution. An inmate retains the right to inspect their PHI
- ☐ The PHI is part of a research study still in progress provided the individual agreed to the temporary suspension of access
- ☐ The PHI was obtained by someone other than a health care provider (e.g., a family member of the individual) under a promise of confidentiality and providing access to the information would be reasonably likely to reveal the source of the information.

Date individual notified: _____ By:_____

Date information provided as requested

☐ Mailed: _____ ☐ Faxed: _____

☐ Emailed: _____ ☐ Placed on patient portal: _____

☐ Picked up in the office: _____ ☐ Other: _____

BREACH/ INCIDENT INVESTIGATION REPORT

Report Date _____ Incident Date _____

Practice Name _____

Practice Address _____

Description of the incident - Describe the incident/use/disclosure with information relevant to how it happened, how it was detected, individuals involved, how it was reported, etc.

_____

_____

_____

_____

_____

Record elements of the investigation – Reports reviewed, people talked to, etc.

_____

_____

_____

_____

_____

Risk Analysis – Answer the following questions to determine status of the incident (Breach or inappropriate use/disclosure).

1. Nature of the event?

Types of PHI involved* Include the amount and type of clinical information released and the nature of the service (mental health, infectious disease)

_____

_____

_____

_____

_____

*Risk increases when credit card/SS info released due to identity theft.

2. Who is the unauthorized person/entity on the receiving end?

Record who the information was released to or accessed by. Was the recipient another CE or BA covered by HIPAA or other privacy rules or an unknown recipient?

_____

_____

_____

_____

_____

_____

3. Was the information actually viewed or simply exposed to a potential breach?

Provide detail on how it was determined which event occurred. For instance audit trail documents access to information in question, mailing returned and unopened or forensic evidence proves data on a computer was never accessed

_____

_____

_____

_____

_____

_____

4. To what extent was the risk mitigated? Mark all that apply.

- ☐ Quick response to the event
- ☐ Information returned
- ☐ Signed confidentiality agreement and PHI being destroyed
- ☐ Additional supporting comments below:

_____

_____

_____

_____

Was the access, use or disclosure ruled a Breach or not? – Describe why the decision was made. The Burden of Proof is on the practice.

Determined not to be a breach for the following reason:

- ☐ Data encrypted
- ☐ Meets one of the following exceptions allowed by the Privacy Rule
    - Unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate. Information is not further used or disclosed in a manner not permitted under the privacy rule.
    - Inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement. Information is not further used or disclosed in a manner not permitted under the privacy rule.
    - Unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- ☐ Signed confidentiality agreement and PHI being destroyed
- ☐ Other reason/Additional details:

_____

_____

Determined to be a breach for the following reason:

_____

_____

_____

For BREACH

Date Patients Notified: _____

Date HHS Notified: _____

Date prominent media outlet informed (list media outlet): _____

For Breaches impacting 500 or more patients, HHS and a prominent media outlet MUST be notified at the same time patients are informed.

NOTE: Attached all supporting documentation to include copy of patient communication.

For Inappropriate Disclosure

Date Accounting of Disclosures entries made in the client record: _____

Corrective action taken or planned to prevent any reoccurrence - Include in this description procedural or system changes made, policies written or changed, sanctions of workforce members, employee training, etc.

_____

_____

_____

The report was prepared by _____

_____ _____

Preparer Signature Date

_____ _____

Privacy Officer Signature Date