Breach is a Four Letter Word

KAREN GREGORY, RN
DIRECTOR OF COMPLIANCE AND EDUCATION
TOTAL MEDICAL COMPLIANCE

1

Important!

Handouts are on the Handouts TAB

On the right side of your screen

You must be REGISTERED and LOGGED IN to receive CE credit

2

Disclaimer

Karen Gregory RN is an employee of Total Medical Compliance.

Karen Gregory is a Hu-Friedy Key Opinion Leader, a consultant for SciCan and serves on the OSAP Board of Directors.

3

Objectives

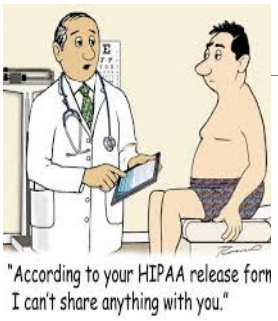
- Recall two examples of recently reported breaches
- Define breach and post event risk analysis guidance
- List three strategies a practice can implement to reduce the likelihood of a breach

4

Important Definitions

- HHS – Health and Human Services
- OCR – Office for Civil Rights
- CE - Covered Entity
- PHI – Protected health information
- ePHI – Protected health information stored electronically.
- BA - Business Associate
- HITECH - Health Information Technology for Economic and Clinical Health

5



What is YOUR greatest risk ?

BREACH

Unauthorized acquisition, access, use or disclosure of unsecured PHI

6

U.S. Department of Health and Human Services
Office for Civil Rights

State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
MO	Healthcare Provider	520	05/24/2019	Hacking/IT Incident	Email
NY	Health Plan	1811	05/24/2019	Unauthorized Access/Disclosure	Paper/Films
IN	Healthcare Provider	106000	05/24/2019	Unauthorized Access/Disclosure	Desktop Computer, Electronic Medical Record, Email, Laptop, Network Server
OH	Healthcare Provider	2433	05/24/2019	Unauthorized Access/Disclosure	Email
MI	Healthcare Provider	978	05/24/2019	Hacking/IT Incident	Network Server
CO	Healthcare Provider	7515	05/22/2019	Hacking/IT Incident	Email
MN	Healthcare Provider	1198	05/21/2019	Hacking/IT Incident	Email
PA	Healthcare Provider	917	05/21/2019	Unauthorized Access/Disclosure	Electronic Medical Record
MT	Healthcare Provider	14794	05/17/2019	Hacking/IT Incident	Email
NC	Healthcare Provider	4450	05/16/2019	Hacking/IT Incident	Network Server
FL	Business Associate	501	05/15/2019	Hacking/IT Incident	Network Server
NC	Healthcare Provider	500	05/15/2019	Hacking/IT Incident	Network Server

7

Identity Theft

the illegal use of someone else's personal information (such as a Social Security number) especially in order to obtain money or credit –Merriam Webster

8

What elements are included in PHI?

Protected Health Info

The Wrong Hands

Medical or Financial Identity Theft

9

All Time High

Settled 10 cases and one judgment

Totaling $28.7 million

OCR Concludes 2018 with All-Time Record Year for HIPAA Enforcement

OCR Concludes 2018 with All-Time Record Year for HIPAA Enforcement – February 7, 2019 OCR has concluded an all-time record year in HIPAA enforcement activity. In 2018, OCR settled 10 cases

10

Date	Name	Amount
Jan. 2018	Filefax, Inc (settlement)	$100,000
Jan. 2018	Fresenius Medical Care North America (settlement)	$3,500,000
June 2018	MD Anderson (judgment)	$4,348,000
Aug. 2018	Boston Medical Center (settlement)	$100,000
Sep. 2018	Brigham and Women's Hospital (settlement)	$384,000
Sep. 2018	Massachusetts General Hospital (settlement)	$515,000
Sep. 2018	Advanced Care Hospitalists (settlement)	$500,000
Oct. 2018	Allergy Associates of Hartford (settlement)	$125,000
Oct. 2018	Anthem, Inc (settlement)	$16,000,000
Nov. 2018	Pagosa Springs (settlement)	$111,400
Dec. 2018	Cottage Health (settlement)	$3,000,000
	Total (settlements and judgment)	$28,683,400

6/5/2019

11

Penalty Range Under HIPAA

For the practice/business associates per year the issue persisted:

- Tier 1: $100-$50,000 per violation, capped at $25,000
- Tier 2: $1,000-$50,000 per violation, capped at $100,000
- Tier 3: $10,000-$50,000 per violation, capped at $250,000
- Tier 4: $50,000 per violation, capped at $1.5 million

For employees:

- $50,000 - $250,000 plus from 1 – 10 years in prison.
- *Intent to sell, transfer, or use phi for commercial advantage, personal gain, or malicious harm* - $250,000, imprisoned not more than 10 years, or both.

12

Examples

$999,000 – Filming without permission

$125,000 – Patient contacted local TV station

$114,000 – Access to scheduling software

13

Lessons Learned

Risk Analysis is required

Access to ePHI must be deleted

Audits must be performed

Policies and procedures current

Encryption utilized

Breach notification must occur

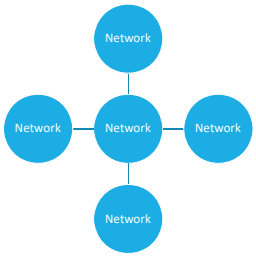
14

Why is HITECH important?

Health Information Technology for Economic and Clinical Health Act

Increased access to ePHI

Sharing of PHI via Health Information Exchanges



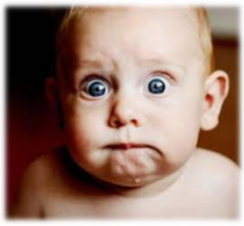
15

Who manages a breach in the practice?

- Patient notification – 60 days
- Must notify HHS
- Notify media for 500 or more impacted records

16

BREACH



17

Events Leading to Breach Scenarios

Workers – Training is imperative
- Curiosity, naive
- Retaliation

Lax passwords or passwords stored inappropriately

Inadequate technology to protect ePHI

Business Associates

Improper disposal of paper and other media

Theft - Building security is a must

Unattended equipment

18

Breach Exclusions

Wrong patient's record

Information shared with wrong worker

Not enough time to retain information

19

Next Steps

- Who to notify *immediately*
- Patients -without reasonable delay and no later than 60 days
- 500 or more: notify media and HHS
- Notification may be costly
  - Reputation
  - Legal claims/lawsuits
  - Action by OCR
  - Worker liability

20

Breach Notification and the BA

- Notify CE no later than 60 days
- Address timing of report in BA contract
- CE ultimately responsible to report
  - May be delegated by contract to the BA
  - Does not lessen the responsibility of the CE
  - Both parties should NOT report

21

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? *Even if all items below are met, the incident may still be a reportable breach*. 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

Breach Notification Template

This template may be used to notify affected individuals of a breach of protected health information. Instructions in italics are requirements from **§ 164.404 Notification to individuals** regarding a breach.

Name of Practice
Address
Phone number

Dear Sir or Madame

This letter is to inform you of a breach of your personal health information.

> *Provide a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known*

The following information was inappropriately accessed or shared:

> A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

We are committed to the protection of your personal information and apologize for this event. The following steps are being taken to prevent this from occurring in the future.

> *A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and*

Please closely monitor your credit reports and investigate and charges to any accounts that you have not authorized.

> *Any steps individuals should take to protect themselves from potential harm resulting from the breach*
> .
> *While not required by regulation, the CE may consider offering credit monitoring.*

Please feel free to contact us with any questions or concerns you may have about this situation. You may reach us (fill in method).

> *Contact procedures for individuals to ask questions or learn additional information, which shall include a toll free telephone number, an e-mail address, Web site, or postal address.*

Sincerely.

Privacy Officer/Site Manager

Complete Risk Analysis

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.

_____

_____

_____

_____

22

Patient Notification Process

- Written notice:
  - First class mail or by electronic mail
  - Multiple mailings
  - May call, followed by written notice
- Incorrect contact info
  - Substitute notice via email
- Incorrect contact for 10 or more:
  - Posting on Web site for 90 days
  - Notice in major print/broadcast media
  - Toll-free number for patient questions

23

Patient Notification to Include

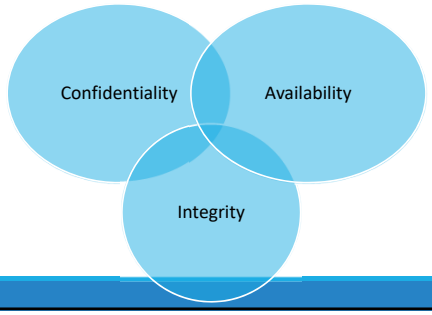
- What happened
- Description of the types of unsecured PHI
- Steps to protect themselves
- What is being done to investigate and repair
- Contact information

24

Protecting Information

25

Security Rule



26

Training

Baseline training for all new employees
- Train specific job functions on targeted areas of need

Priority to train employees regarding breach

Protection strategies
- Minimum necessary
- Logins/passwords
- Computer protections – physical security
- Social media
- Acceptable information sharing sites
- Remote access

27

Minimum Necessary

- Only the amount of PHI necessary to complete the healthcare task
- Access PHI when involved in the care of a patient
- NO access for curiosity reasons

28

Sanctions Policy

All workers will be held accountable to protect PHI

29

Safeguarding ePHI

- Strong IT vendor or IT on staff
- Strong passwords
- Log off or lock computer
- Security updates
- Physical security of computers/devices
- Social media accounts
- Data encryption

30

Risk Analysis and Audits

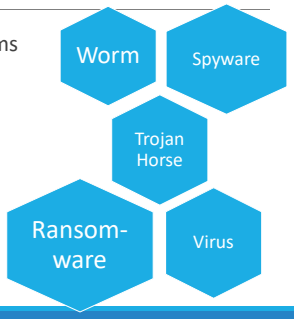
Risk Analysis required by the Security Rule

Audits
- Logons outside business hours
- Remote access report
- File update or change reports
- Review of daily activity
- Employees logged in
- Record access
- Logon when person out of office
- Hard drive audit
- Exceptional access or print
- VIP record access

31

Malware – Behind the Scenes

Damage computer systems and disrupt patient care
- Ensure security updates current
- Open emails only from reliable source(s)
- Don't click on links
- Contact IT for ransomware message



32

Should we worry about HHS?

Date	Name	Amount
Jan. 2018	Filefax, Inc (settlement)	$100,000
Jan. 2018	Fre[illegible] ement)	$3,500,000
June 2018	MD	$4,348,000
Aug. 2018	Bos	$100,000
Sep. 2018	Brig[illegible]	$384,000
Sep. 2018	Massachusetts General Hospital (settlement)	$515,000
Sep. 2018	Advanced Care Hospitalists (settlement)	$500,000
Oct. 2018	Allergy Associates of Hartford (settlement)	$125,000
Oct. 2018	Anthem, Inc (settlement)	$16,000,000
Nov. 2018	Pagosa Springs (settlement)	$111,400
Dec. 2018	Cottage Health (settlement)	$3,000,000
	Total (settlements and judgment)	$28,683,400

Respect

33

Final Thoughts

- Healthcare information is VALUABLE
- Minimum necessary
- Protect your logon information
- If you walk away lock it or log off
- KNOW the location of portable equipment
- Don't CLICK on LINKS
- IT support

34

Thank you!

Karen Gregory, RN
Director of Compliance and Education
www.totalmedicalcompliance.com
Karen@totalmedicalcompliance.com
888.862.6742

35