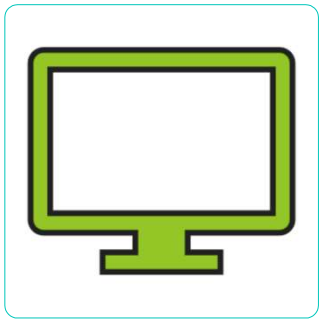


Virtual Privacy Investigations

Chrissy Kyak, CHC, MS Cyber Security & Cyber Investigations

MedStar Georgetown University Hospital, Compliance & Privacy Officer

MedStar Health Research Institute, Director of Research Compliance, Research Integrity Officer, Research Conflict of Interest Officer and GDPR Data Protection Officer

1

Discussion Points for Today's Presentation

- PRIVACY & SECURITY INCIDENT TRENDS
- FORENSIC RESOURCES UTILIZED
- INVESTIGATIONS TOOLKIT FOR MANAGERS
- VIRTUAL INVESTIGATIONS
- THE ANATOMY OF AN INVESTIGATION
- VIRTUAL EDUCATION FOR EMPLOYEES

2

Privacy & Security Incident Trends

3

Privacy Incident Trends – COVID-19

- Viewing COVID-19 test results, without a business reason
- Famous individuals who are inpatient with COVID-19
- Providers who send messages in the EMR directly to a family member to notify them of a positive family member or their own test diagnosis
- Requests from associates to validate whether someone looked in their medical record without a business reason when they have a positive COVID-19 diagnosis
- Managers viewing their employee's electronic medical records
- Questions regarding Occupational Health versus Clinical Information
- Verbal communications

4

Privacy Incident Trends

- Employee access to family member medical record information, including printing or modification
- Requests from associates to validate whether someone looked in their medical record
- Reports from employees, directly or through the hotline, regarding inappropriate EMR access
- Paperwork handed, faxed or mailed to the wrong patient
- Paperwork left unattended

5

Security Incident Trends

- Employees working at home sending emails to their personal email accounts, containing PHI
  - Emails containing spreadsheets with PHI
  - Emails with medical record documentation
- Device theft, including laptops and organization-issued cell phones
- Physical security: PHI left in plain view on monitors, improper disposal of PHI; secure doors left open
- Employees sharing user credentials
- Employees clicking on links embedded in phishing emails
- Malware

6

Survey

What trends in privacy and security incidents are you seeing in your organization since the beginning of COVID-19?

- Paperwork handed to the wrong patient
- Snooping incidents into charts with COVID-19 lab results
- Emails sent to personal email addresses, containing PHI
- Verbal disclosures of PHI
- Malware
- Phishing incidents
- Lost or stolen devices

7

Utilization of Forensic Resources

8

Forensic Tools Utilized for Investigations

Forensic Tools:

Several auditing tools can be utilized to run audit trails in almost real time to review incidents of privacy violations or snooping. (Fair Warning, Maize . . .)

When are these tools used?:

To validate any reported, suspected incidents of inappropriate access from employees

To view findings from standard reports:

- Same Last Name Report
- Same Address Report
- Employee and Patient in same department Report
- Employee and the Patient are the same person (not a HIPAA violation, but in some organizations, a policy violation)

9

Forensic Tools Utilized for Investigations: Information Available in the Audit Trail

- **Who was in the medical record**
- **Whether they live at the same physical address (HR Tables)**
- **Whether they have the same last name**
- **What did the user view**
- **How did they view it – what device were they using**
- **What facility are they working from**
- **Did they print, view or modify the medical record**
- **When was the last time the patient was seen? Did they have an appointment**
- **Were they seen in the viewer's department**
- **ICD-10 and CPT Codes**

10

Forensic Tools Utilized for Investigations
Information Available in your Electronic Medical Records

- Audit Trails
- Treating providers
- Individuals involved in care
- Were they seen by the employee's department?
- Have they been in recently for care?
- Is the employee listed as next of kin or person to contact in the medical record?
- Does the individual that accessed the medical record work at your hospital or facility?

11

Privacy/Compliance Investigations Toolkit for Managers

12

Investigation Toolkit for Managers

Discussion with the manager regarding the process for an investigation is your most important first step in any investigation that involves talking to employees

- Discuss validation of audit findings with manager, if the incident was discovered through your auditing tools

Validate with the manager:

- Is this access part of the employee's regular course of work?
- Did you ask the employee to access this record?
- Is this appropriate access?

You always want to validate first whether the employee accessed for a business reason, as opposed to a personal reason with the manager

13

Investigation Toolkit for Managers

Your investigation plan:

Contact the manager to get their perspective on what is in the audit trail. If the manager does not confirm that this was warranted access:

- Find out the employee's work schedule
- Inform the manager that you would like them to coordinate with the employee to be in the manager's office for the meeting when it occurs
- Ask the manager to keep the investigation confidential. If the employee asks what the meeting is about, it is about "a reported privacy incident."
- Discuss with your Human Resources representative to go over the audit trail and discuss what the findings mean. Don't assume that anyone understands the audit trail. Going over what it says before the employee meeting is crucial.

14

Investigation Toolkit for Managers – Human Resources' Role

Human Resources is a valuable partner in your interview process.

- Meet with them ahead of the interview to go over any questions they have regarding the audit trail or details of the case
- Talk through what will happen if the incident is confirmed to be a substantiated breach or an unsubstantiated breach
- Talk through your **Sanctions Policy** with your Human Resources partner to make sure they are using the policy to apply consistent sanctions for the incident, if sanctions are needed

Your partnership with Human Resources is a crucial part of your investigation plan. Keep them informed of any updates to the case, if there are new developments.

Always follow up with HR to make sure that you close the loop on your investigation – know what corrective action was given if there was a violation.

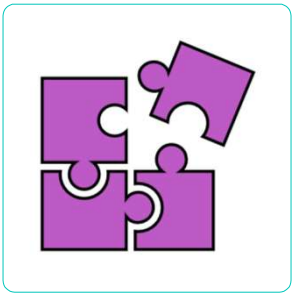
This is an important step in closing out your case.

15

Conducting A Virtual Investigation

16

The Anatomy of an Investigation



Audit Trail Investigations involve

- Audit trail identifies one employee who may have inappropriately accessed a medical record
- Interview of one employee
- Potential corrective action and re-education for employee

Full Investigations can involve

- Interviews of multiple employees
- Interview summaries
- Investigation summary
- Development of a corrective action plan

17

Beginning your Interview: General Advisements to the Employee

Preliminary Advisements:

Thank you very much for your participation here today. Before we start, I would like to go over some background and advisements:

- ✓ This is a comprehensive review into an incident reported in the _____ Department.
- ✓ We conduct reviews of this nature whenever concerns like this come up.
- ✓ You were identified as someone who has first-hand knowledge of relevant, factual information.
- ✓ To ensure accurate factual information and enable us to do the right thing, please keep the content of this meeting confidential. We ask that you please not discuss your interview with others.
- ✓ In addition, there may be other concurrent reviews underway. We work to coordinate with other reviews to ensure efficiency and consistency.

18

General Advisements Continued . . .

- ✓ Our goal today is to gather factual information only. At the end of the interview, you will have the opportunity to ask any questions that you have regarding the investigation.
- ✓ We also ask that you please do not presume any facts or conclusions have been reached because of a question we ask.
- ✓ We have a non-retaliation policy. Retaliation is forbidden by law and policy even if the underlying reported concern cannot be confirmed. If you feel you have been retaliated against for sharing facts with us, please let us know. We also ask that you not seek out or speak to anyone as a result of concerns about anything we ask here today. If you have a question or concern, please feel free to reach out me with your questions.

Do you understand these advisements? Yes

Do you agree to comply with these requests? Yes

Before we begin do you have any questions regarding these advisements? No

19

In-Person versus Virtual Investigations

- Employees are often more relaxed in a virtual meeting as opposed to an in-person investigation.
- The incident is more private – co-workers don't see the Compliance Officer and Director of HR coming into the department, going into the manager's office and seeing what employee is being spoken to.
- Will we continue virtual investigations when employees go back to work?

20

Conducting a Virtual Privacy Investigation

Interview conducted through Microsoft Teams or your preferred virtual platform

Human Resources and Compliance are on the line

The manager is in their office with the employee

General Advisements are given to the employee

If there is an audit trail, we share the document during the meeting to discuss the findings

Scripted questions for larger investigations

Close with a confidentiality statement regarding the discussions during the meeting

Questions? Compliance drops off the line.

HR stays on the line with the manager to provide answers to any questions regarding corrective action or other employee questions regarding next steps.

21

Workforce Sanctions Policy

After the interview – what's next?

- Manager and Human Resources review our workforce sanctions policy, and decide corrective action, if any
- If this was a larger investigation, Compliance develops an investigative summary of:
  - Initial Allegations
  - All individual interviewed
  - Findings
  - Corrective actions
  - Whether the allegations were substantiated or unsubstantiated, based on the investigation findings
  - Close your case
    - A closed case memo is important to memorialize your investigation findings and corrective measures taken

22

Survey Question:

How Would You Handle This Scenario?

Patient leaves the hospital and is handed his discharge paperwork. When he gets home, he realizes he had another patient's paperwork. He notifies the department of the error. The employee self-reports the incident to compliance:

- Treat this incident as a breach, and work with HR to sanction the employee
- Treat this incident as a breach, and thank the employee for reporting the incident to Compliance
- Ask the patient the shred the paperwork, and consider the incident closed

23

Leveraging Technology: Virtual Education for Employees

24

Leveraging Technology for Employee Education

30% of employees entering training with little or no knowledge of the topic that is about to be presented reported that the presentation did not help them understand the subject matter (CEB Gartner)

Get a pulse check on your employees' understanding of compliance topics

- Are you finding that employees just don't know the rules?
- Are employees ignoring the rules or have forgotten them?
- Do your employees know where to find compliance and privacy policies? Do you have an intranet site where they can be found easily?
- Are you seeing any knowledge gaps for employees discovered during investigations?
- Do your employees know that you are the resource to contact for any questions in a compliance or privacy subject area?
- Is your program more reactive or proactive?
- Remember: you need to reach your employees quickly, and make it relative to their role in your organization.

25

Leveraging Technology for Employee Education

All of these areas are reasons to conduct training, but in a COVID environment, you need to get creative and utilize virtual resources.

- **Get buy-in from your leadership and share with them the trends you are seeing in a subject area, and let them know that training would benefit employees**
- **Offer training on Microsoft Teams. During the month of September 2020, I had over 250 people sign up for two sessions of basic HIPAA training**
- **Poll your departments to find out where they feel they could use some resources in the way of training or where they think they may be a little rusty on the rules and policies**

26

Leveraging Technology for Employee Education

What are the organization's expectations?

- Access is only for work. Never use your access for a personal reason
- Never ask another employee to access your medical record so you can view your medical information
- You may not access a family member's medical record or any medical record for a personal reason
- You may not access your own medical record in any business systems (depending on your entity's policy)
- Sign up for the patient portal if you want to access your medical information electronically

27

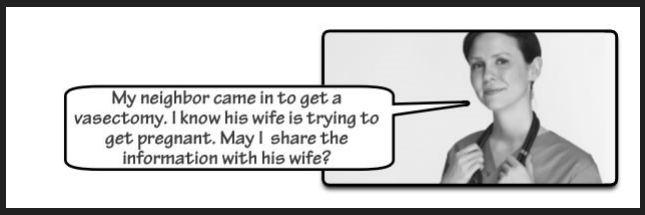
Provide scenarios for your employees to discuss and react to

Looking at a patient's medical record <u>without a business reason</u> is a violation of the HIPAA Privacy Rule.

- Scenarios:
  - My mother was in the emergency room over the weekend. I want to look at her record and print her a copy. She's thinking of contacting a lawyer.
  - My son has an appointment coming up, and I want to validate the date and time.
  - My brother had an MRI. I want to know the results. He said it was ok to look.
  - My co-worker is missing a lot of work. I want to know why.
  - I need to scan some documents and change my family's insurance information. I'll just do it myself.
  - I work in labor and delivery. I want to know how my co-worker's high-risk pregnancy is going. I can go into her record, because I work in labor and delivery. Did I mention she is only 12 weeks pregnant?

28

Is It Permissible to Use or Share Protected Health Information?



Permissible: Treatment
Permissible: Payment
Permissible: Operations
Not Permissible

Permissible: Treatment
Permissible: Payment
Permissible: Operations
Not Permissible

Give scenarios in different formats. These scenarios give the employees the opportunity to answer and give the right response to these scenarios

29

Is It Permissible to Use or Share Protected Health Information?

Permissible: Treatment
Permissible: Payment
Permissible: Operations
Not Permissible

Permissible: Treatment
Permissible: Payment
Permissible: Operations
Not Permissible

30

Use Videos, Infographics and Graphics to Convey Information Security Rule – Physical Security

1 Identify a "secure area" in the picture.

Physical security areas that could create HIPAA risks or breaches

31

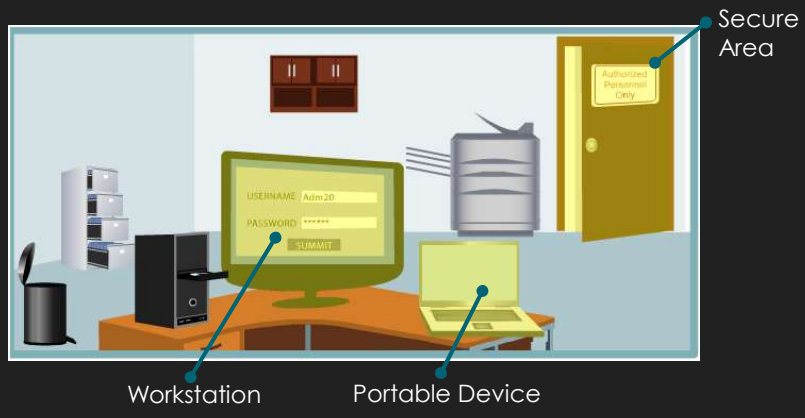
Minimize Physical Security Risks to Protect Confidential Information

2 Identify a "workstation" in the picture.

32

Minimize Physical Security Risks to Protect Confidential Information

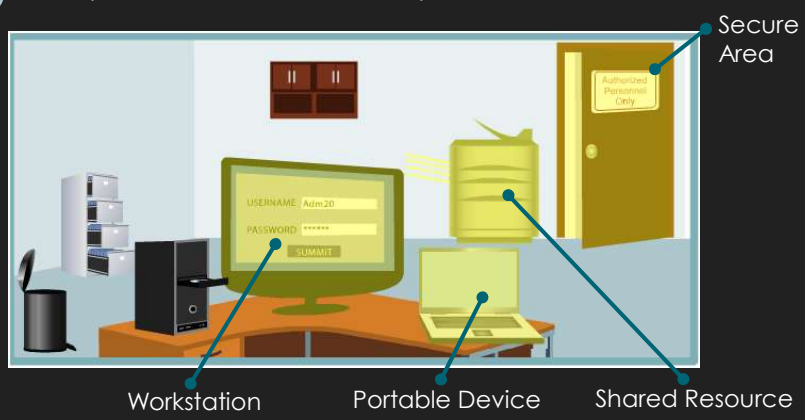
3 Identify a "portable device" in the picture.



33

Minimize Physical Security Risks to Protect Confidential Information

4 Identify a "shared resource" in the picture.



34

Minimize Physical Security Risks to Protect Confidential Information

5 Identify a place to "dispose of information" in the picture.

35

Who is Your Contact When You have Questions about Privacy?

Chrissy Kyak

Your Title

Your Entity

Phone/Cell

Christine.R.Kyak@_____

Want to Report a Compliance Issue Anonymously?

Contact the Anonymous Hotline

1 (877) _____

An anonymous line operated by a third-party vendor (24/7)

36

Thank you for attending this presentation!

If you have any questions regarding this presentation, please feel free to contact me:

Chrissy Kyak, CHC
Compliance & Privacy Officer
MedStar Georgetown University Hospital
Director of Compliance, Privacy & Research Integrity Officer
MedStar Health Research Institute
(202) 510-6876
Christine.R.Kyak@Medstar.net

37

Questions?

38