IS IT A BREACH?

Scott T. Gima, RN, BSN, MHA
Executive VP & COO
Management Performance Associates
Today’s Topics

• Breach definition
• Breach statistics and trends
• Social media
• Verbal PHI
• Disposal of physical PHI
• Lost PHI
• Paper PHI
• Other unauthorized access/disclosures
• Ransomware cyberattack
Breach Defined
What is a Breach?

An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

• The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

• The unauthorized person who used the protected health information or to whom the disclosure was made;

• Whether the protected health information was actually acquired or viewed; and

• The extent to which the risk to the protected health information has been mitigated.

HIPAA Breach Statistics and Trends
Office of Civil Rights – Enforcement Statistics

13 Civil Monetary Penalty Cases (CMPs)

Total Resolutions: 26,420

- Resolved after Intake and Review
- Post-Investigated Technical Assistance
- Investigated: Corrective Action Obtained
- Post-Investigated Technical Assistance
- Investigated: No Violation

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html#ir2021
As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

**Cases Currently Under Investigation**

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

**Breach Report Results**

<table>
<thead>
<tr>
<th>Expand</th>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Iowa Department of Health and Human Services</td>
<td>IA</td>
<td>Health Plan</td>
<td>833</td>
<td>05/26/2023</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>✔️</td>
<td>Lancaster Orthopedic Group</td>
<td>PA</td>
<td>Healthcare Provider</td>
<td>500</td>
<td>05/26/2023</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>✔️</td>
<td>UI Community Home Care, a subsidiary of University of Iowa Health System</td>
<td>IA</td>
<td>Healthcare Provider</td>
<td>67897</td>
<td>05/24/2023</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record, Network Server</td>
</tr>
<tr>
<td>✔️</td>
<td>Grant Regional Health Center</td>
<td>WI</td>
<td>Healthcare Provider</td>
<td>4135</td>
<td>05/23/2023</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
</tbody>
</table>

Source: [https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)
OCR Breach Portal Reports

HEALTHCARE DATA BREACHES OF 500 OR MORE RECORDS

Hacking Unauthorized Access/Disclosure Loss/Theft Improper Disposal

OCR Reports - Breach Type
2009 - 2022

Type of Breaches
OCR Breach Portal Archive Data

Source: [https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)
Location of Breaches
OCR Breach Portal Archive Data

Source: [https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)
OCR Breach Portal Statistics
Covered Entities or Business Associates
2009 - 2022

OCR Breach Types 2021
Under 500 and Over 500 Reports

Breach Type – Under 500
- Unauthorized access/disclosure: 94%
- Loss/Theft: 3%
- Hacking/IT: 1%
- Improper disposal: 1%

Breach Type – 500 and Over
- Unauthorized access/disclosure: 16%
- Loss/Theft: 5%
- Hacking/IT: 78%
- Improper disposal: 1%

OCR Breach Location 2021
Under 500 and Over 500 Reports

Breach Location – Under 500
- Paper 70%
- EMR 12%
- Email 5%
- Desktop/laptop 1%
- Other 10%
- Server 1%

Breach Location – 500 and Over
- Server 70%
- Email 26%
- EMR 2%
- Other 2%

Social Media in the News
Chicken Coop Social Media Post – Is it a Breach?

• EMS workers responded to a man who collapsed in a chicken coop.
• After the visit, an EMS worker posted a message on Facebook about the incident. The message was – “well, we had a first ... We worked a code in a chicken coop! Knee deep in chicken droppings.”
• Additional comment added to the post by the EMS worker: “it was awful” and “I’m pretty sure y’all could smell us in dispatch.”
• No PHI was mentioned.

Chicken Coop Social Media Post – Is it a Breach?

• The county attorney does not believe HIPAA has been violated, but did say that the post should not have been made on social media.

• Wife: “Even though she did not mention his name, she said it was the first time they had ever had a call in a chicken coop. Everybody knows where my husband died.”

It is a good idea to have a social media policy
Yelp Review – Is it a Breach?

Patient:

“Both teeth Dr. XXXXXX did root canals on failed and had to be extracted. DO NOT let him go through the gum like he did with both of mine. Never heard of this before and it is pretty obvious doesn’t work. Just makes $$$ for him.” “Stay away!!!!”

Response by Dentist:

I attempted multiple times to contact you so we could handle our concerns in private. You chose to put your grievances on an open forum which means now by law you have forfeit your right to the doctor/patient confidentiality act. I regret that I must proceed with this openly.
Yelp Review – Is it a Breach?

Dental practice fined $23,000 and 2 year monitored Corrective Action Plan

OCR Director, Melanie Fontes Rainer quoted in the press release:

• “This latest enforcement action demonstrates the importance of following the law even when you are using social media. “Providers cannot disclose protected health information of their patients when responding to negative online reviews.”

• “OCR is sending a clear message to regulated entities that they must appropriately safeguard patients’ protected health information. We take complaints about potential HIPAA violations seriously, no matter how large or small the organization.”

Sign up for OCR updates. [https://www.hhs.gov/ocr/list-serv/index.html](https://www.hhs.gov/ocr/list-serv/index.html)

Another Yelp Review

Manasa Health Center - $30,000 CMP – June 5, 2023
Small psychiatry practice
- Disclosed the PHI of a patient in response to their negative online review.
- OCR’s investigation found three additional online review disclosures and no HIPAA Privacy policies and procedures.
- OCR Director Melanie Fontes Rainer: “OCR continues to receive complaints about health care providers disclosing their patients’ protected health information on social media or on the internet in response to negative reviews. Simply put, this is not allowed.”

Verbal PHI
Background

• RN assisting an echocardiogram technician and physician in performing a transesophageal echocardiogram.

• While conducting a “time out” procedure, RN verbally informed her colleagues that they should wear gloves because the patient has Hepatitis C.

• Patient filed a HIPAA breach complaint alleging improper disclosure of PHI as the RNs voice was loud enough to be heard by other patients and/or medical personnel who were nearby.
Verbal PHI Breach?

• The hospital suspended then terminated the RN for the HIPAA violation.

• RN sued the hospital for wrongful termination based on:
  • There was no HIPAA violation
  • At most, she engaged in "incidental disclosure" which is not actionable under HIPPA

Source: https://www.cnn.com/2023/03/02/us/california-embryo-cancer-gene-lawsuit/index.html\
Verbal PHI Breach?

Wrongful termination case thrown out by lower court and upheld by the Appellate Court

• Nurse cannot rely on HIPAA as a basis for a wrongful discharge claim. HIPAA's confidentiality provisions exist to protect patients, not healthcare employees

• The court agreed that a medical provider must use the minimum amount of protected health information to accomplish the necessary purpose. 45 C.F.R. 164.502.

• The court concluded that, "under HIPAA, nurses’ statement was not the minimum amount necessary to accomplish the warning.

Source: Hereford v. Norton Healthcare, Inc. d/b/a Norton Audubon Hospital and Phyllis Vissman
Disposal of Physical PHI
Paper PHI on the Side of the Road

• A motorist stops and finds nursing home prescription records on the side of the road.

• PHI: name, birth date, SSN, address, pharmacy information, nursing home information, medication name and dosage.

• The nursing home states that the records were given to a third-party shredding vendor

• Who is responsible for the breach? Nursing home or shredding company?
If a third-party vendor (shredding company) commits a breach, the covered entity is responsible for investigating and reporting the breach.

- Identify all business associates - vendors and consultants that touch, create, transport or destroy your PHI and ePHI.
- Business Associates Agreement (BAA) are required for each
- For BAA, consult an attorney
- Key issues:
  - Notification requirements
  - Indemnification

• New England Dermatology practice was disposing empty patient specimen bottles in regular trash for 10 years

• The bottles contained the patient’s first and last names, dates of birth, the date on which the specimen was taken, the name of the provider who took the specimen, and the general area of the body from which the specimen was taken
Specimen Bottles in Trash

• Self reported
• **OCR settlement on August 23, 2022 for $300,640 and a Corrective Action Plan**
  • Destruction method makes PHI unreadable, indecipherable, and otherwise **cannot be reconstructed**
  • Paper records: shredding, burning, pulping, or pulverizing
  • Specimen bottles: Store in **opaque bags** in a **secure area** and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHOCR disposal

OCR FAQ [https://www.hhs.gov/sites/default/files/disposalfaq.pdf](https://www.hhs.gov/sites/default/files/disposalfaq.pdf)

Sources:
Lost PHI
• Casco Bay EyeCare

• A USB drive containing the protected health information (PHI) of 1,432 individuals was lost.

• The PHI involved included names, dates of birth, and diagnoses.
Lost ePHI

• Casco Bay EyeCare

• A USB drive containing the protected health information (PHI) of 1,432 individuals was lost.

• The PHI involved included names, dates of birth, and diagnoses.

• After reporting to the OCR, the USB drive was found and OCR closed the case.

TIP! Encrypted USB drives that are lost or stolen = no breach

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
Paper PHI in the News
Patient Records Stolen from Truck

• Oct 2020. Coast Dental.
• A locked moving truck was stolen from a parking lot in Atlanta, GA.
• It contained equipment and patient records for a dental practice.
• Police recovered the truck within 24 hours.
• Approximately 1,700 patient records were compromised or missing.

Source: https://www.coastdental.com/about/press-releases/notice-to-our-patients
Patient Records Stolen from Truck

• Oct 2020. Coast Dental.
• A locked moving truck was stolen from a parking lot in Atlanta, GA.
• It contained equipment and patient records for a dental practice.
• Police recovered the truck within 24 hours.
• Approximately 1,700 patient records were compromised or missing.
• Coast Dental notified HHS, affected individuals, the media, and posted a substitute notice on its website.
• Mitigation: Implemented additional physical safeguards

Source: https://www.coastdental.com/about/press-releases/notice-to-our-patients
Not the Best Use of Recycled Paper
Is it a Breach?

- A patient went to the hospital for a blood pressure check
- The nurse recorded the BP on the back of a recycled piece of paper
- The patient noticed patient PHI on the backside of the paper
- The backside showed a patient’s name, address and positive HIV status

Source: https://www.dailymail.co.uk/news/article-10791417/Shoalhaven-Hospital-patients-details-leaked-piece-scrap-paper-used-nurse.html
Not the Best Use of Recycled Paper

Source: https://www.dailymail.co.uk/news/article-10791417/Shoalhaven-Hospital-patients-details-leaked-piece-scrap-paper-used-nurse.html
Heightened Attention to Sensitive PHI

• In 2014, a hospital employee accidently faxed information to the individual's employer instead of sending to the patient's PO box.

• The PHI included sensitive information concerning HIV status, medical care, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis and physical abuse.

• $387,000 OCR settlement agreement for a 2 record breach (the hospital had a similar earlier incident)

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/stlukes/index.html
Unauthorized Access/Disclosure
Email Sent to Wrong Person – Is it a Breach?

- Nov 2022. Yakima Neighborhood Health Services (State of Washington)

- Staff member inadvertently sent the protected health information (PHI) of 2,689 individuals to the wrong recipient.

- The recipient deleted the file.

- No evidence that any information potentially involved in this incident has been misused.

Email Sent to Wrong Person – Is it a Breach?

• Incident was reported to the OCR.
• YNHS also contacted affected individuals, the media, and posted substitute notice on its website.
• YNHS responded to the breach by conducting additional privacy and security training to its workforce members, implemented additional technical safeguards, and revised its policies and procedures.

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
Dental Practice – Sharing Passwords

• Feb 2023. Troy Roeder DDS.
• Employees shared their passwords
• Affected protected health information (PHI) of 1,127 individuals

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
Dental Practice – Sharing Passwords

• Feb 2023. Troy Roeder DDS.
• Employees shared their passwords
• Affected protected health information (PHI) of 1,127 individuals
• Sharing passwords is impermissible – unique credentials required
• In response to OCR’s investigation, additional technical and physical safeguards were implemented, policies and procedures revised, and employees retrained on the HIPAA Privacy Rule.
• OCR provided technical assistance to the CE regarding its relevant Security Rule obligations.

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
Ransomware
Cyberattacks
Ransomware Attacks in the News – Big Ones

• May 23, 2023. MCNA Dental Insurance. At least 8.9 million individuals were affected. Current and former members of certain state Medicaid and Children’s Health Insurance Programs

• Apria Healthcare - Home medical equipment provider. 2 million individuals affected during data breaches that occurred in 2019 and 2021.

• PharMerica - National pharmacy network. 5.8 million individuals impacted from a March 2023 data breach.
Ransomware Attacks in the News – Smaller/Rural Ones

- La Clinica de La Raza ("La Clinic"), Oakland CA. Employee email accounts accessed over a two-week period. 15,316 affected.
- Two Rivers Health Department. One employee’s Office365 account accessed between September 14 and November 8, 2022. 15,168 affected.
- Skin MD - cosmetic and laser skin care provider. Paper records were stored in a protected, off-site storage center. Some were found discarded non-securely after someone reported it to the police. 7,758 affected.
- Morris Hospital & Healthcare Centers, an 89-bed hospital located 55 miles southwest of Chicago
- Idaho Falls Community Hospital, 88-bed hospital – clinic closed, ambulance diversions

Central Control Corporation – debt collection company
Located in Newport News, VA
March 2023 incident impacting at least 286,000 individuals

<table>
<thead>
<tr>
<th>VCU Health System</th>
<th>UVA Health System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valley Health System</td>
<td>Sentara Health System</td>
</tr>
<tr>
<td>Riverside Health System</td>
<td>Bayview Physicians Group</td>
</tr>
<tr>
<td>Mary Washington Healthcare,</td>
<td>Pariser Dermatology Specialists, Inc.</td>
</tr>
<tr>
<td>Chesapeake Regional Medical Center</td>
<td>Tidewater Physicians Multispecialty Group</td>
</tr>
<tr>
<td>Dominion Pathology Laboratories,</td>
<td>Chesapeake Radiology</td>
</tr>
<tr>
<td>Children’s Hospital of the King’s Daughters Health System and its Affiliates</td>
<td></td>
</tr>
</tbody>
</table>
Is A Cyberattack a Breach?

Maybe.............??????

• Is there evidence that data was not viewed or exfiltrated (acquired)?
• Audit logs?
• Report to OCR?
  • Amount of affected individuals
  • Type and amount of data breached
Hospital Cyberattack

• October 28, 2020. University of Vermont Medical Center
• First signs - applications stopped working
• Malware installed on over 5,000 workstations and laptops
• 1,300 servers encrypted
• Revenue loss of about $64 million or roughly $1.5 million per day

Cause of Cyber Attack

• An employee took a corporate laptop on vacation and opened a personal email from his homeowners association

• When the email was opened, malware was installed on the laptop.

• The hospital attack began when the employee returned to work and connected to the Medical Center network

Source: https://vtdigger.org/2021/07/21/malware-on-employees-company-computer-led-to-cyber-attack-on-uvm-medical-center/
Cyber Attack Recovery

• Good backups were in place
• Usual initial response – everything taken offline
• It is a time consuming task to wipe every computer, laptop and server and reinstall software/applications and data
• My rough estimate: 2 hours per computer to wipe and reinstall operating system equals 10,000 man hours or 417 calendar days working 24/7
• Don’t forget: Manual data entry for medical records and billing
• Two months after the attack, 80% of the hospital's applications were restored, representing 98% of hospital function even with additional help provided by Vermont National Guard Cyber Team

OCR – Investigation Trends

OCR’s *Report on Breaches of Unsecured Protected Health Information*

Frequently found non-compliance issues:

- **Risk Analysis.** An accurate and thorough assessment of the potential risks and vulnerabilities to the electronic PHI (ePHI) held by the covered entity or business associate.

- **Risk Management.** Implementation of sufficient security measures to reduce potential risks and vulnerabilities to a reasonable and appropriate level.

- **Information System Activity Review.** Record, store and review information system activity, such as audit logs, access reports, and security incident tracking reports.

- **Access Control Standard.** A covered entity must implement technical policies and procedures that allow only authorized persons to access ePHI.

Privacy Rule
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

Security Rule
https://www.hhs.gov/hipaa/for-professionals/security/index.html

Breach Notification Rule
https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Security Risk Assessment Tool
Questions?

Scott Gima, RN, MHA
COO, Executive VP of Compliance & Management
Management Performance Associates
314.394.2222 ext. 121
12155 Old Big Bend Road, Suite 303
Kirkwood, MO 63122
stg@healthcareperformance.com

This presentation is not legal advice.