Monthly HIPAA News

OCR Patient Right of Access Enforcement

The OCR entered three settlement agreements with dental practices for HIPAA Patient Right of Access violations:

Family Dental Care, P.C.

- What happened:
  - Former patient requested a complete set of records on May 8, 2020, but only received partial records.
  - Patient filed a complaint with the OCR on August 8, 2020.
  - All of the requested records were eventually provided on October 12, 2020.
- HIPAA issue: Failure to provide timely access to records (in most cases, 30 days from date of request)
- Result: $30,000 settlement and corrective action plan

Great Expressions Dental Center of Georgia, P.C.

- What happened:
  - Patient requested her records on November 25, 2019.
  - GEDC-GA required a $170 copying fee.
  - GEDC-GA did not provide records due to copy fee non-payment.
  - Complaint filed with the OCR on November 4, 2020.
  - Medical records finally provided on February 2, 2021.
- HIPAA issues: Failure to provide timely access; copying fees that were not "reasonable and cost-based."
- Result: $80,000 settlement and corrective action plan

B. Steven L. Hardy, D.D.S.

- **What happened:**
  - **April 11, 2020 - patient emailed the provider a request for access to copies of her and her minor child's PHI.**
  - **April 14, 2020 - the provider sent a reply email to the patient explaining that the office was closed and offered to email the requested PHI to her if the patient confirmed her email address.**
  - **May 4, 2020 - patient sent a confirmation email to the provider.**
  - **After patient made several subsequent requests, the provider required patient to submit a written request with her handwritten signature before it would provide the requested PHI.**
  - **December 4, 2020 - Patient submitted a written request with her handwritten signature.**
  - **December 31, 2020 - Provider sent patient copies of her and her minor child's PHI, eight months after the initial request.**
- **HIPAA issue: Failure to provide timely access**
- **Result: $25,000 settlement and corrective action plan**

What we can learn from the Patient Right of Access settlements:

- **These three patient right of access cases brings the total to 41.**
- **The OCR expects all providers to respond timely to records requests, including large hospital systems as well as small providers such as dental practices.**

HIPAA Breach Class Action Settlements

Ambry Genetics

- **Settlement amount: $12.25 million class action settlement**
- **Nature of breach: Hacker accessed one email account. Emails and attachments contained ePHI.**
- **Size of breach: 200,000 individuals**
- **Allegation: Failure to implement cybersecurity measures to protect PHI**
- **OCR action: No information provided on OCR breach portal.**

ClearBalance

- **ClearBalance is a business associate that services hospital and other provider loans made to patients who need to finance medical expense payments.**
- **Settlement amount: $2.65 million**
- **Nature of breach: Unauthorized party accessed employee email accounts. The ePHI found in the emails included names, addresses, drivers' license numbers, Social Security numbers, diagnoses, and financial information.**
- **Size of breach: 200,000 individuals**
- **Allegation: Failure to prevent breach; failure to inform individuals in a timely fashion; failure to protect systems from third parties.**
- **OCR action: Provided technical assistance regarding its security management process.**

Social Media News

Therapy llama. A video of a "therapy llama" visiting nursing home residents made the news. Residents pet and fed the llama – and the video, which included residents, brought a lot of positive comments. Remember: therapy llamas in nursing homes are cute, but every resident captured in the video must have signed a valid HIPAA authorization before the video was taken.

Unauthorized photographs. A Kansas man sued a hospital for permitting a Reuters photographer to photograph him while he was using a ventilator and fighting COVID-19. The plaintiff claims he could not consent to the photos because he was incapacitated, and his wife did not give permission.

Cyber Stats: Ransomware is a patient safety issue

Proofpoint recently published the following study, conducted by The Ponemon Institute: Cybersecurity in Healthcare: The Cost and Impact on Patient Safety and Care. The study identified the following statistics for organiztions that had experienced a ransomware attack:

- **24% reported an increase in the mortality rate**
- **48% reported an increase in complications from medical procedures**
- **50% reported an increase in patient transfers to other facilities**
- **59% reported longer lengths of stay**
- **64% reported delays in procedures and tests that resulted in poor outcomes.**

Breach News Roundup

Every month, there are far more breaches than we have space to share! Trends include: unauthorized access to email; phishing; cyberattacks; ransomware/malware; and unauthorized access by employees. Here are a few examples:

Stolen USB drive

- **Who: Montefiore Medical Center**
- **What happened: A research coordinator's USB storage device was stolen.**
- **PHI involved: Patient demographic and clinical information**

Business associate breach: law firm

- **Who: Warner, Norcross & Judd LLP**
- **What happened: An unauthorized party accessed the network. Note: The breach notice was published more than nine months after the incident (HIPAA requires 60 days).**
- **PHI involved: Name, DOB, SSN, driver's license number, other IDs, credit card information, patient account number, health information, and more**

Deleted files

- **Who: First Street Family Health**
- **What happened: A cyber-attack deleted electronic PHI, including some backups.**
- **PHI involved: Name, DOB, address, phone number, email address, SSN, dates of service, nature of services including diagnoses, conditions, lab results, medications, health insurance ID cards and numbers, and billing information**

From the Blog

Is HIPAA the Key to Customer Service?

By Margaret Scavotto, JD, CHC

The way a healthcare provider handles HIPAA can be the difference between a patient coming back and giving you a good review – or walking out the door and posting their bad experience on social media.

Example 1

A patient calls to tell you they received a letter with information for another patient.

How the employee answering the phone responds can make the difference between a good outcome – and an unhappy customer who submits a complaint to the Office for Civil Rights.

Does your compliance team train receptionists to thank the person for calling, and keep them on the line until you can get a supervisor – or, better yet, the Privacy Officer, on the phone? Does the receptionist give the caller the direct number of the Privacy Officer in case they get disconnected? Or does the person who answers the phone direct the call to someone else, where the caller gets voicemail, and starts to get frustrated and thank your organization doesn't care?

Example 2

A nurse aide takes a video with patients in the background and posts it on TikTok. Are your employees trained to know that this is a potential HIPAA breach? Will they immediately notify the Compliance Officer or Privacy Officer? Or is it possible that your employees will "like" the video, and share it to a few co-workers? How fast your organization hears about – and mitigates – these issues determines how many patients or potential patients learn about them.

Example 3

A potential patient walks into your organization for the first time.
Do they overhear PHI? Do they see PHI on monitors? A few months ago I was referred to a new doctor. While in the patient room (alone), I could see a TV screen next to my chair, showing the name of every other patient who had an appointment that week – and the reason for the appointment. On my way out, I saw X-rays on a tv screen at the reception area, and I could see patient names on the X-rays. I did not go back. Would you?

Example 4

It wouldn't be a HIPAA blog if we didn't mention TikTok. A few weeks ago, a friend of mine who also works in healthcare and who loves a good HIPAA horror story, sent me a TikTok video. A woman is telling viewers that she recently went to the doctor for some tests, and on the intake form, there was a box asking if the doctor's office could share test results with her husband. The patient checked the "No" box. The doctor's office did not call the patient. They called her husband and gave him the test results. When the patient called the doctor's office to discuss this, the doctor

was defensive.

This video has 538,100 likes, 21,700 comments, and 1,584 shares. Here are some of the comments:

"this is a textbook HIPAA violation. Like they'd put this in the training of 'what not to do.'"
"you definitely could report her for violating [HIPAA]"
"You might need to consider a lawyer"
"I would report simply to avoid it happening to someone in bad situations"
"After that attitude I would switch Doctors...immediately"

I didn't read all 21,700 comments, but... you get the idea. Every one of the comments I read was a strong negative reaction to the doctor's office. They understand their privacy rights. Privacy is important to everyone. Social media has the potential to exponentially amplify one mistake into a huge public relations nightmare.

Example 5

Let's end with a positive example. A few years ago I had an outpatient surgical procedure. I provided my driver's license, I was given an ID bracelet, and throughout the check-in process, my personal information was verified multiple times. Not once did they ask for or say my name out loud. Not once was my identity revealed to anyone else nearby. This hospital went beyond what HIPAA requires to show me even more respect than is required by law. Surgery is no fun – but feeling respected helps. . And because I appreciate the way I was treated, I want to pay it forward and let everyone know that Missouri Baptist Medical Center truly understands patient privacy.

If you elevate the way your organization treats privacy, patients will feel appreciated. They will come back. And they will tell other people wonderful things about you – in an online review, around the dinner table, or on their blog.

Patient Specimens Thrown Out In the Trash - Are You the Last to Know?

By Margaret Scavotto, JD, CHC

Is your HIPAA training program identifying new risks?

The OCR recently announced a $300,640 HIPAA settlement with New England Dermatology, P.C., d/b/a/ New England Dermatology and Laser Center (NDELC), for "improper disposal of protected health information."

In 2021, NDELC filed a breach report regarding its self-discovery that it discarded empty specimen containers with PHI on the labels in the parking lot garbage bin, for ten years.

MPA blogged about the specimen bottle in July 2021. We've included it in our HIPAA trainings for healthcare employees ever since.

Are you staying ahead of the news and addressing new risks in your training?

Are you overlooking PHI?

PHI exists beyond the medical record. It includes patient names written on a rounding whiteboard. It includes data surrounding your medical devices. It also includes specimen bottles with labels containing patient information. And yet, I think we can all relate to the specimen bottle story – sometimes, we just forget something. Because much of the focus is on ePHI breaches, it is easy to forget that paper or physical PHI breaches don't happen very often, but they still happen. The purpose of your HIPAA program is to prevent that from happening to you.

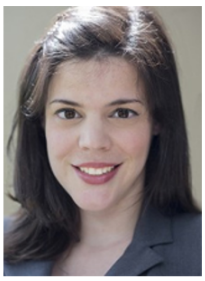
Create a PHI inventory.

This process fits naturally with your HIPAA Security Risk Analysis. A PHI inventory is simply a list of every kind of PHI in your organization: electronic and paper, stored, transmitted, received, and created. The PHI inventory will include obvious sources like the EHR, computers, networks, and flash drives. The PHI inventory should include less obvious sources, too, like PHI handled by a business associate – and even specimen containers

When it comes to the PHI inventory, more heads are better than one. You might think of something I missed. Get your Compliance Committee together for a brainstorming session. Every time the Committee meets, ask again: do we have any new sources of PHI? Are we sharing or using PHI in a new way?

Like the HIPAA Security Risk Analysis, the PHI inventory should be updated regularly (and whenever you add a new form of PHI!). Likewise, HIPAA training should extend beyond clinical staff so that all employees are able to identify PHI.

MPA can help you create current HIPAA training. We can also help you develop a HIPAA PHI inventory, and complete a HIPAA Security Risk Analysis.



Margaret Scavotto, JD, CHC
President
Management Performance Associates
314.394.2222 ext. 124
12166 Old Big Bend Road, Suite 303
Kirkwood, MO 63122
mcs@healthcareperformance.com

Scott T. Gima, RN, MHA
Executive VP & COO
Management Performance Associates
314.394.2222 ext. 121
12166 Old Big Bend Road, Suite 303
Kirkwood, MO 63122
stg@healthcareperformance.com