HIPAA update May 2024

Key Concepts

- Privacy Rule
- Examples of Covered Entities and Business Associates
- HITECH Act of 2009
- Minimum Necessary Rule
- 21st Century Cures Act: "Open Notes"
- Common Misconceptions of what is or isn't permissible
- Data on National Cases reported/investigated by Office of Civil Rights
- Penalties
- Summary of VMG Investigations from 2023

HIPAA Privacy Rule

- Obligation to Protect Patient Privacy
- Continuous Review "privacy practices and systems"
- Obligation to protect against unauthorized DISCLOSURES
  - According to HIPAA, disclosure is the release, transfer, or divulging of information outside of the entity that holds it. This can include providing access to the information in any way
- Privacy Rules apply to "Covered Entities" and their "Business Associates"

Privacy Rule (Continued)

- Disclosures for TPO: **T**reatment, **P**ayment, and healthcare **O**perations are permitted *without* consent
  - But, minimum necessary information disclosed
- Enforcement is no longer just "Complaint-driven"
- How investigations may begin:
  - Consumer complaint to Office of Civil Rights (OCR)
  - OCR compliance review
  - OCR audit
  - VMG audit

Examples of Business Associates and Covered Entities

Covered Entities:

- Health plans
- Hospitals
- Healthcare providers
- Medical Practices
- Medical Billing and Claim Service organizations
- Pharmacies
- Durable Medical Equipment providers
- DMH/DMR service provider organizations

Business Associates:

- Lawyers
- Accountants
- Consultants (i.e., experts in legal cases, I.T. consultants, management consultants)
- Managers /Admin personnel
- Contract personnel
- Vendors
- Covered Entities with shared patients

Example of HIPAA Breach Settlement of Business Associate

HHS Office for Civil Rights Settles HIPAA Investigation with Arkansas Business Associate MedEvolve Following Unlawful Disclosure of Protected Health Information on an Unsecured Server for $350,000

May 16, 2023: MedEvolve, a business associate, that provides practice management, revenue cycle management, and practice analytics software services to covered health care entities settled a breach. The settlement concludes OCR's investigation of a data breach, where a server containing the protected health information of 230,572 individuals was left unsecure and accessible on the internet. In addition to the Breach, the OCR found that the HIPAA violations in this case included the lack of an analysis to determine risks and vulnerabilities to electronic protected health information across the organization, and the failure to enter into a business associate agreement with a subcontractor.

Overview of HITECH Act (2009)

- Extension of HIPAA to business associates
- "Minimum necessary" standard for compliance
- Prohibition on sale of Protected Health Information ("PHI")
- Restrictions on marketing
- Increased enforcement & penalties
- Requires affirmative notification of breach

Compliance With "Minimum Necessary" Standard of the HITECH ACT

- You may access patient PHI but only if necessary for your work with "this patient"
- We must make reasonable efforts to limit access to minimum necessary information
- Only those who "need to know" should receive PHI as result of notification or communication workflows.

Example of HIPAA Investigation settled due to Violation of "Minimum Necessary Standard"

Snooping in Medical Records by Hospital Security Guards Leads to $240,000 HIPAA Settlement

June 15, 2023: Yakima Valley Memorial Hospital in Washington settled a breach that affected 419 patients. In May 2018, OCR initiated an investigation of Yakima Valley Memorial Hospital following the receipt of a breach notification report, stating that 23 security guards working in the hospital's emergency department used their login credentials to access patient medical records maintained in Yakima Valley Memorial Hospital's electronic medical record system without a job-related purpose. The information accessed included names, dates of birth, medical record numbers, addresses, certain notes related to treatment, and insurance information. In addition to the fine, Yakima Valley agreed to take steps to bring their organization into compliance with the HIPAA Rules, and will be monitored for two years by OCR to ensure compliance with the HIPAA Security Rule.

Examples of Permitted Disclosures for Intended Purposes:

- For public health purposes

  Example: Reporting positive lab tests as mandated by DPH

- For purpose of medical treatment

  Example: Referrals to Specialist outside of VMG

- Investigations by legal/regulatory authorities

  Example: Board of Medicine Complaint; CMS billing audit

- Reviews of complaints about compliance

  Example: Responding to a Grievance filed by a patient with their Health Insurance

Confidentiality of Family Member's Records

- It is VMG policy that staff and providers should not be accessing their own medical record or those of their family members/relatives
- VMG staff and providers who need access to family member's medical records should gain access via the normal patient approval process
  - Patient family member completes HIPAA authorization form allowing access
  - If appropriate patient family member grants shared portal access
- HIPAA authorization by a family member does not grant VMG employee/provider direct access to that chart- access to information should happen as it would for any other patient who has granted family members access to share medical info

Obligation to Secure PHI

- PHI Secure vs. Unsecure
- Secure=
  - Encryption
  - Proper storage and Destruction
  - Password protection on devices that store PHI- this includes: smart phones/laptops/computers/Voicemail
- Unsecure= PHI that is not rendered unusable, unreadable or indecipherable

Example of Violation Settlement for Social Media Disclosure

HHS Office for Civil Rights Reaches Agreement with Health Care Provider in New Jersey That Disclosed Patient Information in Response to Negative Online Reviews

June 5, 2023: OCR announced a settlement with Manasa Health Center, LLC, a health care provider in New Jersey that provides adult and child psychiatric services. The settlement resolves a complaint received by OCR in April 2020, alleging that Manasa Health Center impermissibly disclosed the protected health information of a patient when the entity posted a response to the patient's negative online review. Manasa Health Center paid $30,000 to OCR and will undertake a corrective action plan that will be monitored for two years by OCR to ensure compliance with the HIPAA Privacy Rule.

Scope of Notification in Event of Unauthorized Disclosures

- Health Care Organizations have an obligation to notify both patients and authorities
- The number of patients with information involved in the breach triggers the scope of notification:
  - Less than 500 patients: Create log and report each breach event annually to HHS
  - More than 500 patients: Notify HHS immediately
- Method of Notification: First class mail (or by email if preference is specified) within 60 days of discovery (or date breach should have been discovered)

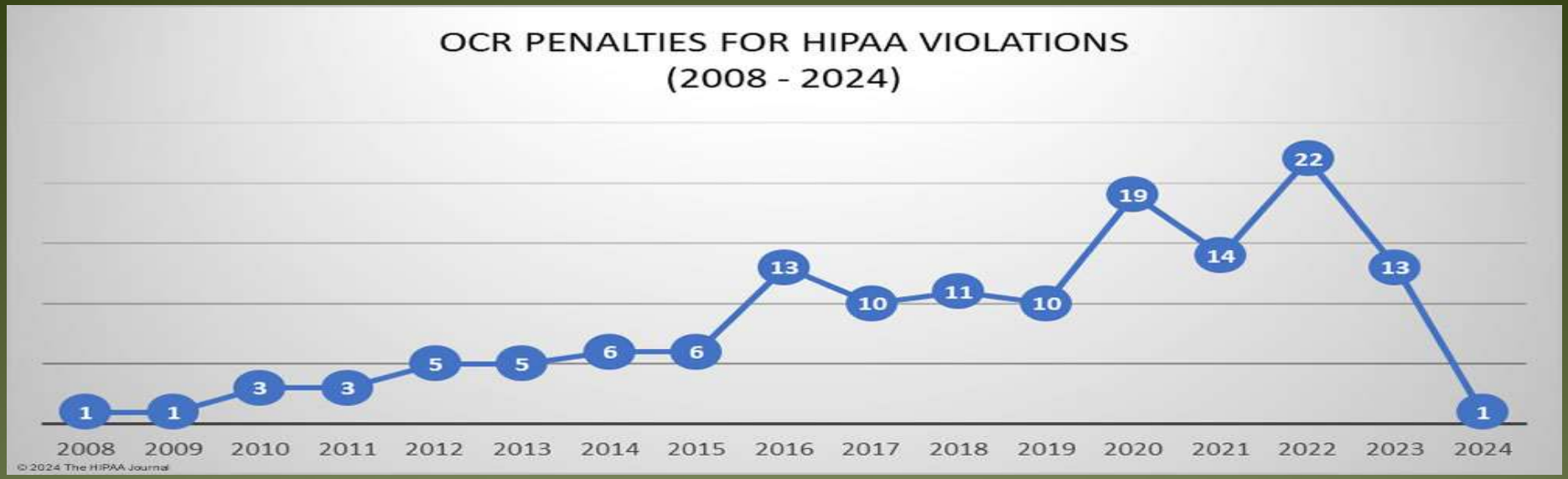
21st Century Cures Act

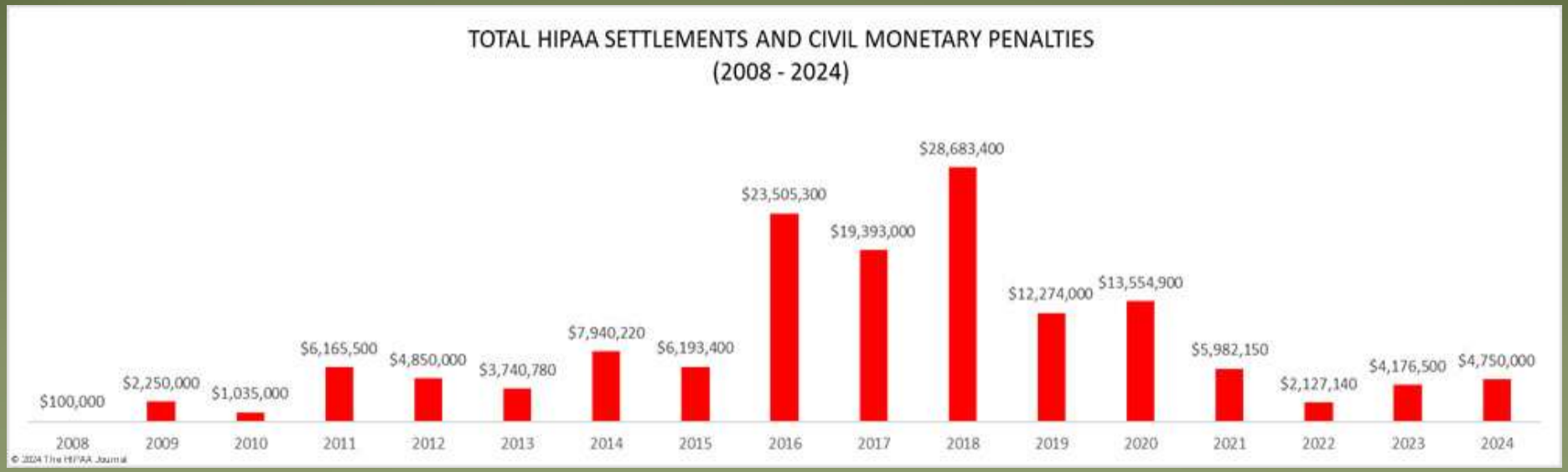
- Requires Healthcare Actors (Healthcare Providers/Healthcare IT developers and EMR companies/Health Information Exchanges) to comply with new Information Blocking regulations
- EMR systems required to adopt new Interoperability with Application Programming Interfaces (API) that allow patients to access, exchange, or use Electronic Health Information (EHI).
- New info blocking regulations are directive and require Actors to provide access, exchange, and use of EHI for nearly all requests.
- Sometimes referred to as Open Notes- this includes records available in the EMR that were not produced by that healthcare provider/medical practice!

Common HIPAA Misconceptions:

- Leaving messages on Answering machines- ***Yes you can!,*** however, be cautious of the content of any message left when the voicemail service does not name the person it belongs to.
- Releasing Information/speaking to family members with verbal consent- ***Yes you can!,*** but document the verbal consent in the EMR and what was consented to release and to who.
- Giving patients documents in the VMG chart that were not from VMG services/produced by VMG provider- ***Yes you can!,*** in fact not complying may be a violation of the 21st Century Cures Act Information Blocking regulations
- Calling police for patient safety or behavior concerns- ***Yes you can!,*** safety of other patients, employees and visitors always trumps concerns for confidentiality

National Data





Adjusted HIPAA Violation Fines (2023)

	Annual Penalty Limit	Minimum Penalty per Violation	Maximum Penalty per Violation	Annual Penalty Cap
Tier 1	Lack of Knowledge	$137	$34,464	$34,464
Tier 2	Reasonable Cause	$1,379	$68,928	$137,886
Tier 3	Willful Neglect	$13,785	$68,928	$344,638
Tier 4	Willful neglect (not corrected within 30 days	$68,928	$68,928	$2,067,813

Tier 1: A violation that a Covered Entity or Business Associate was unaware of and could not have realistically avoided had a reasonable amount of care been taken to comply with HIPAA.
Tier 2: A violation that a Covered Entity or Business Associate should have been aware of but could not have avoided even with a reasonable amount of care to comply with HIPAA.
Tier 3: A violation suffered as a direct result of "willful neglect" in cases where a Covered Entity or Business Associate has been an attempt made to correct the violation.
Tier 4: A violation of HIPAA attributable to willful neglect, where no attempt has been made to correct the violation by a Covered Entity or Business Associate.
Source: https://www.hipaajournal.com/hipaa-violation-fines/

2023 VMG HIPAA Violations

Number of Investigations: 11 Total Violations: 7

Breakdown by center

- AMC 2
- EHC 1
- GHC 2
- NHC 2

Breakdown by department

- **AMC ASPC 1**
- **AMC Referrals 1**
- **EHC Family Practice 1**
- **GHC Billing 1**
- **GHC Health Information Vendor 1**
- **NHC Family Practice 1**
- **NHC Reception 1**

Who is managing this at VMG?

- Compliance Committee
  - Privacy Officer: Amy Rice
  - Compliance Officer: Paul Carlan MD
  - Security Officer: Amy Rice
  - Data Security Officer: Ray Rossini

BUT, we are all responsible to safeguard and protect patients protected health information!

You can report concerns to your supervisor, on an incident report or email qualityreporting@vmgma.com