HIPAA update March 2023

In the dark days, before doctor-patient confidentiality.

"The lab accidentally faxed your test results to the wrong doctor's office. You'll get a bill for a second opinion."

"Somehow your medical records got faxed to a complete stranger. He has no idea what's wrong with you either."

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 2022

HIPAA Privacy Rule

- Obligation to Protect Patient Privacy
- Continuous Review “privacy practices and systems”
- Obligation to protect against unauthorized DISCLOSURES
- 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

9/23/2020: HIPAA Business Associate Pays $2.3 Million to Settle Breach Affecting Protected Health Information of Over 6 million Individuals. CHSPSC LLC provides a variety of business associate services, including IT and health information management, to hospitals and physician clinics indirectly owned by Community Health Systems, Inc., in Franklin, Tennessee. Between April and August 2014, The hackers used compromised administrative credentials to remotely access CHSPSC's information system through its virtual private network, accessing the protected health information of 6 million patients.

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”

A complainant, who was both a patient and an employee of the hospital, alleged that her protected health information (PHI) was impermissibly disclosed to her supervisor. OCR’s investigation revealed that: the hospital distributed an Operating Room (OR) schedule to employees via email; the hospital’s OR schedule contained information about the complainant’s upcoming surgery. While the Privacy Rule may permit the disclosure of an OR schedule containing PHI, in this case, a hospital employee shared the OR schedule with the complainant’s supervisor, who was not part of the employee's treatment team, and did not need the information for payment, health care operations, or other permissible purposes. The hospital disciplined and retrained the employee who made the impermissible disclosure. Additionally, in order to prevent similar incidents, the hospital undertook a complete review of the distribution of the OR schedule. As a result of this review, the hospital revised the distribution of the OR schedule, limiting it to those who have “a need to know.”

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

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 Improper Disposal of PHI

8/23/22: OCR announced a settlement with New England Dermatology P.C., d/b/a a New England Dermatology and Laser Center ("NDELC"), over the improper disposal of protected health information. Empty specimen containers with protected health information on the labels were placed in a garbage bin in their parking lot. The containers' labels included patient names and dates of birth, dates of sample collection, and name of the provider who took the specimen. As a result, NEDLC paid $300,640 to OCR and agreed to implement a corrective action plan to resolve this investigation. NEDLC is located in Massachusetts and provides dermatology services.

Scope of Notification

- Obligation to notify authorities and patients
- Number of patients information involved in the breach triggers 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)

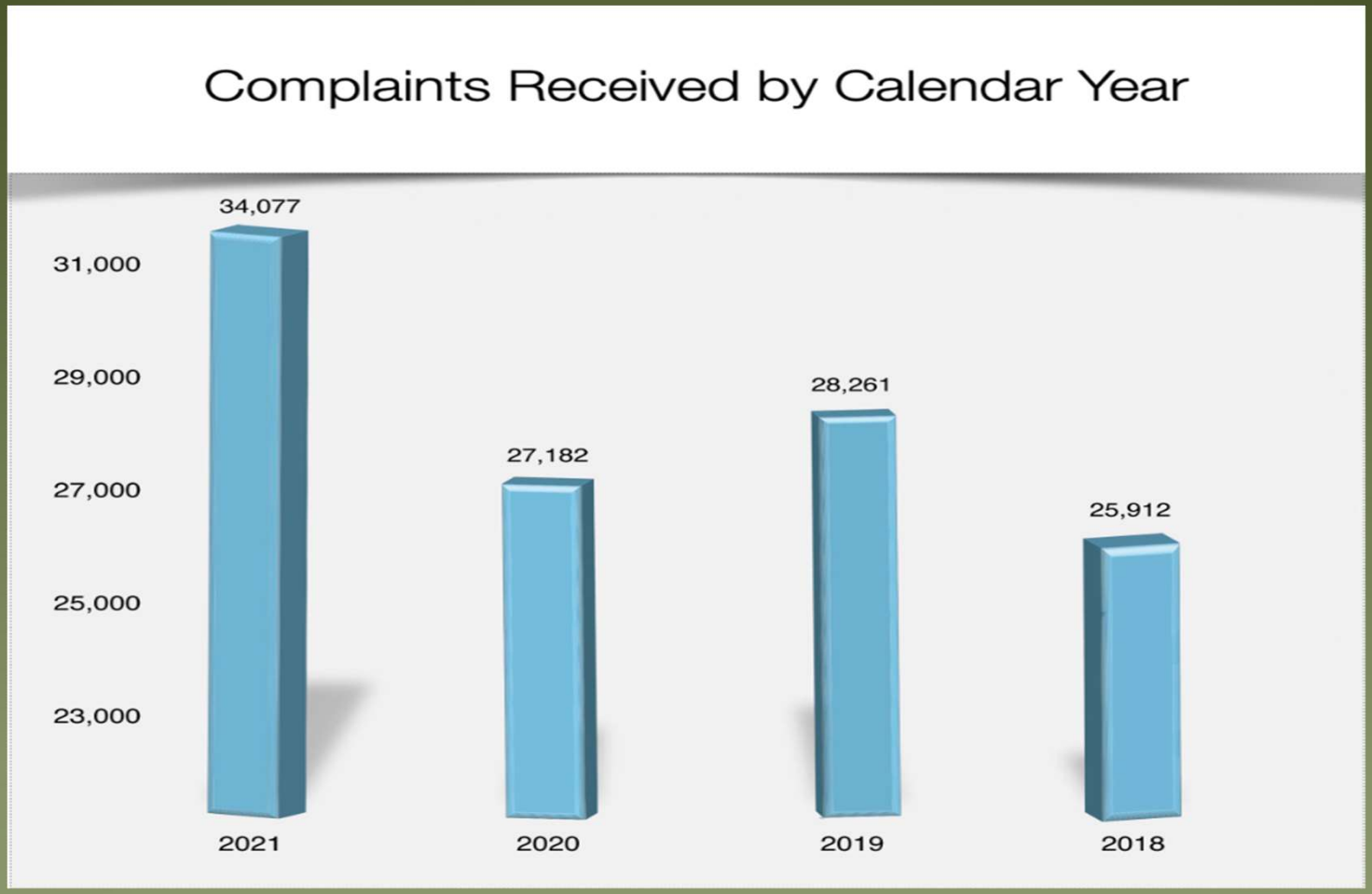
21st Century Cures Act

- 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:

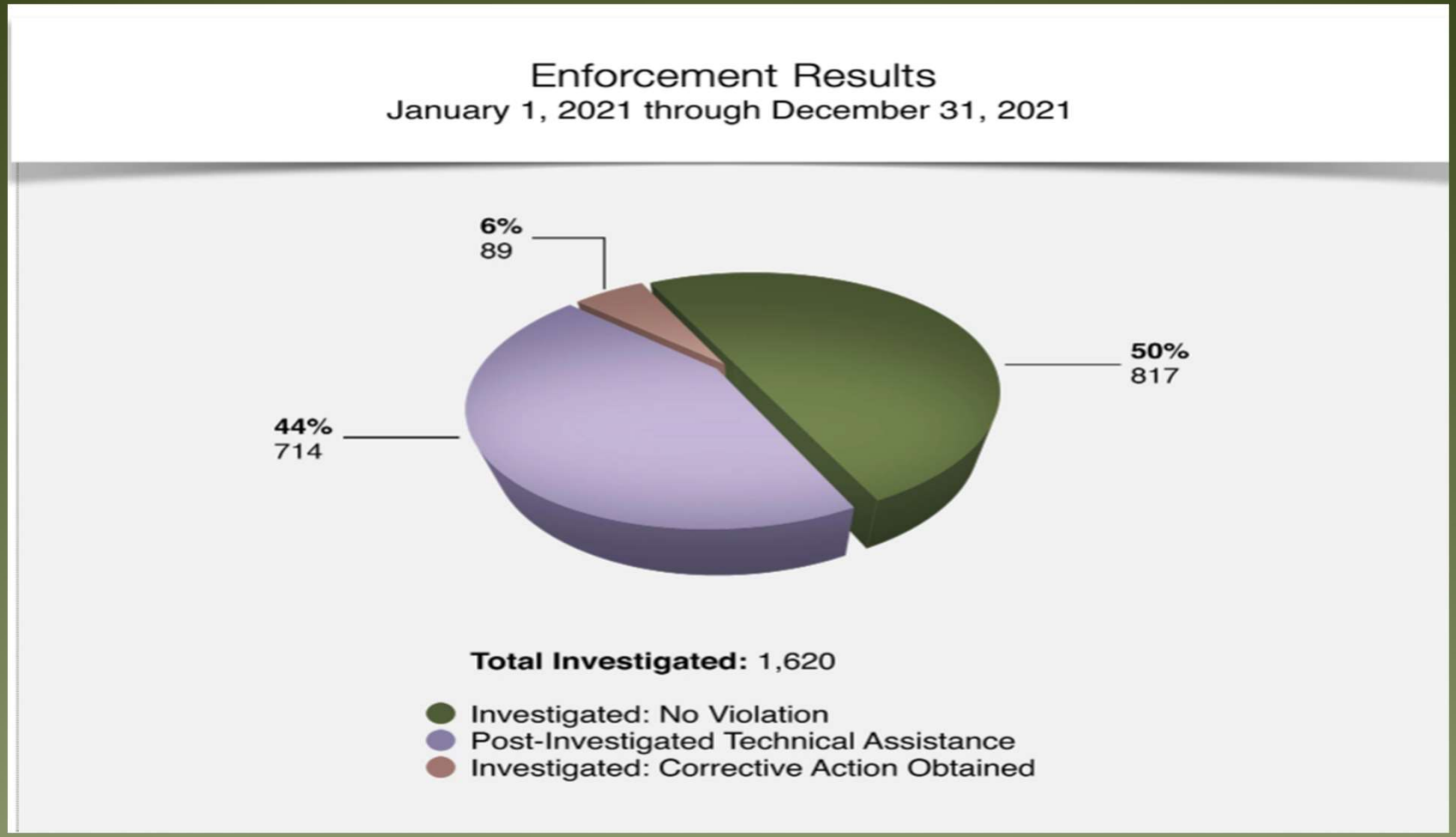
- Leaving messages on Answering machines- ***Yes you can!,*** however, be cautious of the content of any message left when the voicemail service does not name the person it belongs to.
- Releasing Information/speaking to family members with verbal consent- ***Yes you can!,*** but document the verbal 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 of HIPAA Complaints filed with OCR 2018 through 2021



Source: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/complaintsyear.html

National Data of HIPAA Investigations in 2021 By Office of Civil Rights



Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html

Civil Penalties :

- $100 minimum penalty per violation, no cap
- No longer a cap on penalties if the Covered Entity did not know, or even could not have known, of the violation
- Higher penalties based on facts and circumstances of violation

Criminal Penalties:

Criminal Penalties:

- Minimum possible $50,000 and/or up to 1 year prison
- If false pretense found: $100,000 and/or up to 5 years prison
- If gained financial or personally from breach: $250,000 and/or up to 10 years prison

2022 VMG HIPAA Violations

Number of Investigations: 11 Total Violations: 8

Breakdown by center

- AMC 0
- EHC 2
- GHC 6
- NHC 0

Breakdown by department

- EHC Reception 1
- EHC Family Practice 1
- GHC Health Info (vendor) 1
- GHC Outreach 5

Most common HIPAA violation at VMG continues to be mailing documents to the wrong patient.

Who is managing this at VMG?

- Compliance Committee
  - Privacy Officer: Amy Rice
  - Compliance Officer: Henry Simkin
  - 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