HIPAA update December 2021

Key Concepts

- Privacy Rule
- HITECH Act of 2009
- Minimum Necessary Rule
- Review of number of complaints reported nationally
- Penalties
- Review of VMG Cases from 2020
- Review of National Cases/Penalties

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

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 – HITECH Extends HIPAA

- 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

In Order to Comply with Regulations We Must Assure:

- Disclosures are based on intended purpose:
  - For public health purposes
  - For purpose of medical treatment
  - Investigations by legal/regulatory authorities
  - Enforcement efforts by appropriate authorities
  - Reviews of complaints about compliance
  - Patient or authorized representative request

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

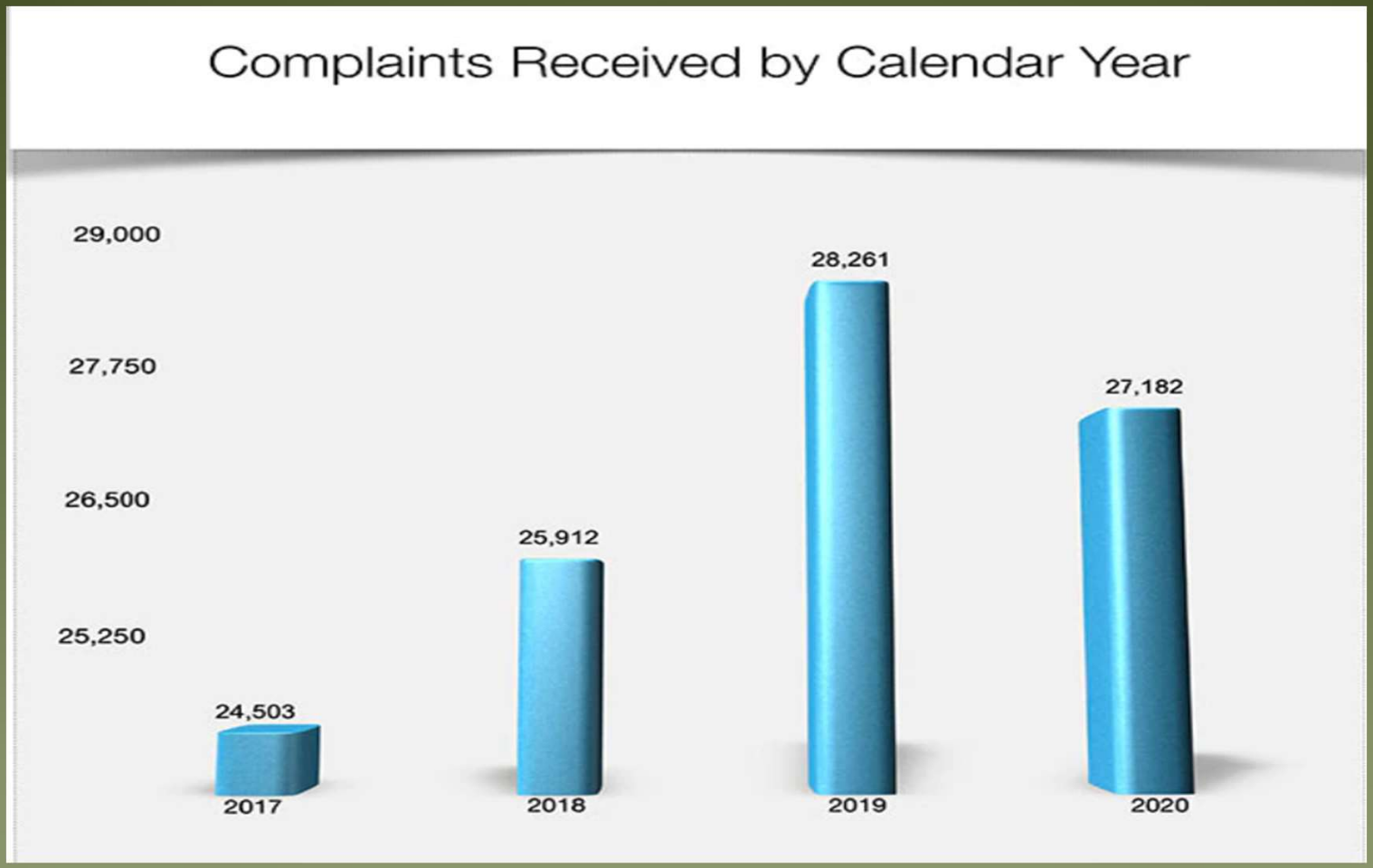
Scope of Notification

- Obligation to notify authorities and patients
- Number of people triggers scope of notification:
  - Less than 500: Create log and report annually to HHS
  - More than 500: 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)

Obligation to Notify if PHI Breach

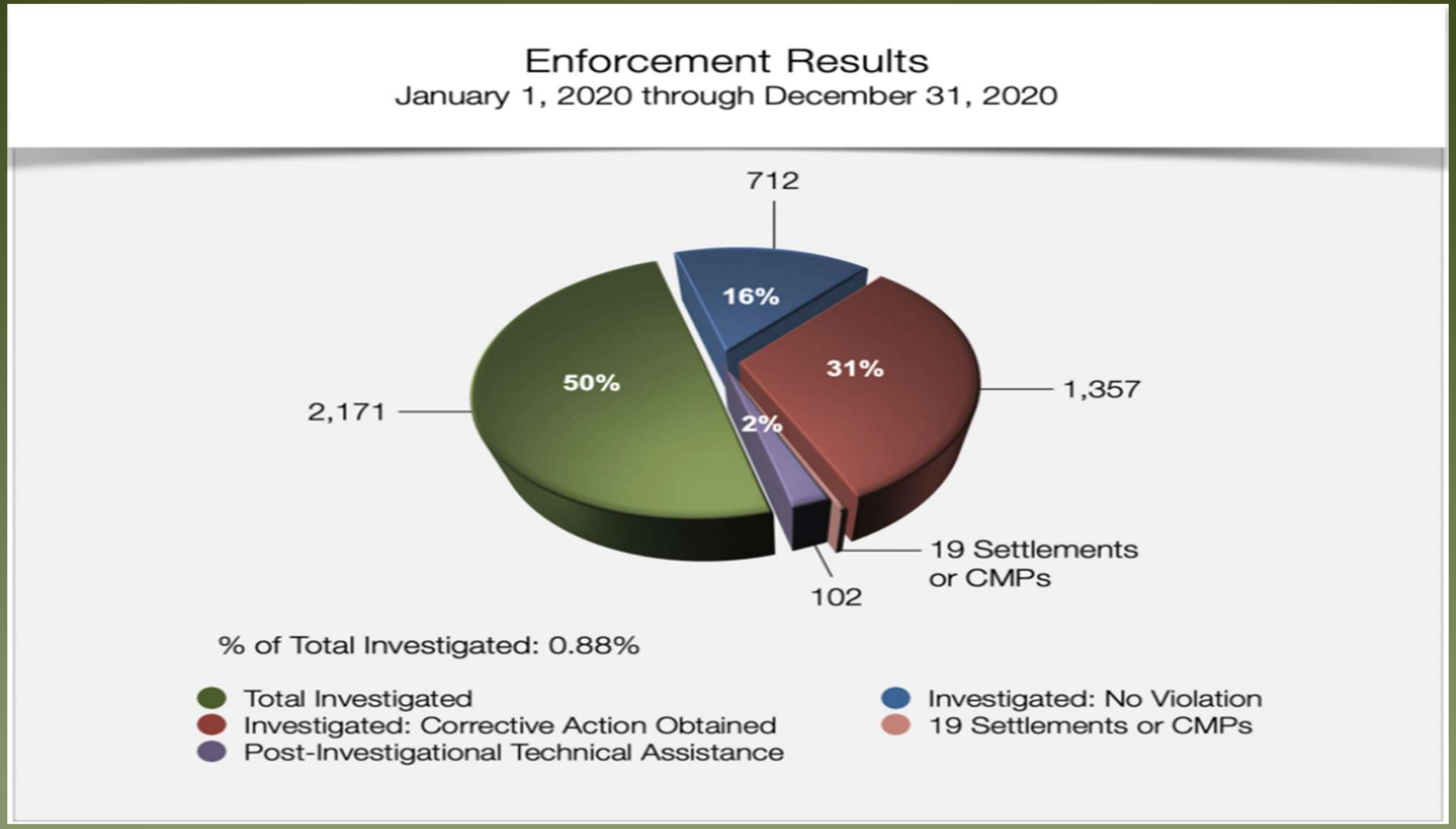
- Date and circumstances of breach
- Date of discovery
- Type of PHI involved
- Steps individuals should take
- Steps Covered Entity is taking
- How the individual can obtain additional information about the breach

National Data on HIPAA Complaints



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

National Data on HIPAA Investigations 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

2020 VMG HIPAA Violations

Number of Investigations: 15 Total Violations: 8

Breakdown by center

- AMC 2
- EHC 0
- GHC 5
- NHC 1

Breakdown by department

- AMC Endocrinolgy 1
- AMC Reception 1
- GHC Endocrinology 1
- GHC Family Practice 2
- GHC Physical Therapy 1
- GHC Reception 1
- NHC FP 1

Trends of VMG Violations

- Demographics errors: wrong email/phone number: 2
- Mailed out lab results to wrong patient: 1
- Faxing error (wrong provider/ fax number) 2
- Other error with wrong patient info used during care/task 3

VMG Cases
(Reported to HHS for 2020)

- Gave patient a urine sample kit that was actually already used and turned in for processing with another patient's sample inside.
- Started to conduct a telephone visit and discuss medical conditions with the wrong person due having the wrong phone number on file.
- Mailed lab reports to the wrong patient
- PHI faxed in error with another patient's document.

National Cases

- September 2020: Orthopedic Clinic Pays $1.5 Million to Settle Systemic Noncompliance with HIPAA Rules
  - Athens Orthopedic is located in Georgia and provides orthopedic services to approximately 138,000 patients annually. On June 26, 2016, a journalist notified Athens Orthopedic that a database of their patient records may have been posted online for sale. On June 28, 2016, a hacker contacted Athens Orthopedic and demanded money in return for a complete copy of the database it stole. Athens Orthopedic subsequently determined that the hacker used a vendor's credentials on June 14, 2016, to access their electronic medical record system and exfiltrate patient health data.

- July 2020: Lifespan Pays $1,040,000 to OCR to Settle Unencrypted Stolen Laptop Breach
  - On April 21, 2017, Lifespan Corporation, the parent company and business associate of Lifespan ACE, filed a breach report with OCR concerning the theft of an affiliated hospital employee's laptop containing electronic protected health information (ePHI) including: patients' names, medical record numbers, demographic information, and medication information. The breach affected 20,431 individuals. OCR's investigation determined that there was systemic noncompliance with the HIPAA Rules including a failure to encrypt ePHI on laptops after Lifespan ACE determined it was reasonable and appropriate to do so. OCR also uncovered a lack of device and media controls, and a failure to have a business associate agreement in place with the Lifespan Corporation.

National Cases (continued)

- November 2019: Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement by University of Rochester Medical Center
  - URMC filed breach reports with OCR in 2013 and 2017 following its discovery that protected health information (PHI) had been impermissibly disclosed through the loss of an unencrypted flash drive and theft of an unencrypted laptop, respectively. OCR's investigation revealed that URMC failed to conduct an enterprise-wide risk analysis; implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; utilize device and media controls; and employ a mechanism to encrypt and decrypt electronic protected health information (ePHI) when it was reasonable and appropriate to do so.

- October 2019: Dental Practice Pays $10,000 to Settle Social Media Disclosures of Patients' Protected Health Information
  - On June 5, 2016, OCR received a complaint from an Elite patient alleging that Elite had responded to a social media review by disclosing the patient's last name and details of the patient's health condition. OCR's investigation found that Elite had impermissibly disclosed the protected health information (PHI) of multiple patients in response to patient reviews on the Elite Yelp review page. Additionally, Elite did not have a policy and procedure regarding disclosures of PHI to ensure that its social media interactions protect the PHI of its patients or a Notice of Privacy Practices that complied with the HIPAA Privacy Rule. OCR accepted a substantially reduced settlement amount in consideration of Elite's size, financial circumstances, and cooperation with OCR's investigation.

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!