
HIPAA PRIVACY
AND SECURITY
TRAINING

# What is HIPAA?

## Health Insurance Portability and Accountability Act

August 1996 - Federal law enacted

↓

April 2001 - Privacy Rule

↓

February 2010 - Security Rule - HITECH Act

↓

March 2013 - HIPAA Omnibus (Final) Rule

↓

2023- Proposed Rule Changes (not yet approved)

# Why must your College comply HIPAA?

Your college is a member of FCSRMC and FCSRMC is self-insured for your group health insurance.

A self-insured group health plan is one in which the employer assumes the financial risk for providing healthcare benefits to its employees as opposed to purchasing a “fully-insured” plan from an insurance carrier.

FCSRMC has retained the services of Florida Blue, as a Third-Party Administrator (TPA), to administer your health benefits.

# Why must your College comply with HIPAA?

FCSRMC and its member colleges are a Covered Entity under HIPAA because you have an employer-sponsored group health plan with more than 50 participants.

## Examples of a Group Health Plan include:

- ✓ Hospital and Medical Benefit Plans
- ✓ Dental Plans
- ✓ Vision Plans
- ✓ Prescription Drug Benefits
- ✓ Health Flexible Spending Accounts (FSAs)
- ✓ Health Reimbursement Accounts (HRAs)
- ✓ Employee Assistance Programs
- ✓ Wellness Programs
- ✓ Disease Management Programs
- ✓ Cancer Policies

# Covered Entity

HIPAA defines a Covered Entity as health plans, health care clearinghouses, and health care providers who electronically transmit health information in connection with transactions concerning billing and payment for services or insurance coverage.

## Health Care Providers

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies
- Hospitals
- Labs
- Imaging Centers

## Health Plans

- Health Insurance Companies
- HMOs
- Company Health Plans
- Government programs that pay for health care such as Medicare, Medicaid, Tricare, and Veterans health care programs

## Health Care Clearinghouse

- Includes entities that process nonstandard health information they receive from another entity into a standard electronic format. The Clearinghouse receives claim information from the provider/hospital and transmits the information to the insurance carrier

# Business Associate

A **Business Associate** is a person or entity that performs certain functions or activities that involve the use or disclosure of Protected Health Information (PHI) on behalf of, or provides services to, a Covered Entity.

**Business Associates include:**

* Benefit Management Company
* Document Storage Company
* Collection Agency
* Attorney
* CPA Firm/Accountant
* Consultant
* I.T. Vendor
* Data Transmission Service

**Business Associates do not include:**

* Healthcare Provider
* Janitor Service
* Electrician
* U.S. Postal Service
* Private Courier
* Construction Worker

Business Associates are accountable for protecting the privacy/security of PHI and are directly liable for criminal and civil penalties for violations.

# Protected Health Information (PHI)

Protected Health Information (PHI) is any information held by a Covered Entity which concerns health status, the provision of healthcare, or payment for healthcare that can identify an individual.

We are required to protect a person's privacy when collecting, using, storing, disclosing, transmitting, and disposing of PHI in verbal, written, or electronic form (including photos and videos).

HIPAA regulations list 18 different personal identifiers:

- Names
- All geographical data smaller than a state
- Dates (other than year) directly related to an individual
- Telephone Numbers
- Fax Numbers
- E-Mail Address
- Social Security Number
- Health Plan Beneficiary Number
- Medical Record Number
- Account Number
- Certificate/License Number
- Vehicle Identifiers (License Plate Number)
- Device identifiers and serial numbers
- Web URLs
- IP Address
- Biometric Identifiers (retinal scan, fingerprint)
- Full Face Photographic Images
- Any Other Unique Identifying Number/ Code

# De-Identified Health Information

De-identified health information refers to information that cannot be used to identify an individual. Examples include information that has been redacted from documents containing health information, or reports that do not identify a specific individual.

Uses:

- Research (market analysis)
- Financial Reports
- Statistical Reports
- Demographic Information
- Reports for Public Health Purposes
- Quality Improvement Activities
- Health Care Operations

# HIPAA Privacy Rule

**Establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, healthcare clearinghouses, and healthcare providers that conduct certain healthcare transactions electronically.**

**Requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.**


**Gives patients' rights over their health information, including rights to examine and obtain a copy of their health records and to request corrections.**

# Notice of Privacy Practices

The HIPAA Privacy Rule states that an individual has a right to adequate notice of how a covered entity may use and disclose protected health information, as well as his or her right to privacy, and the covered entity's obligations with respect to any information that is stored. Most covered entities must develop and provide individuals with this notice of their privacy practices.

A group health plan that does not create or receive PHI other than a summary or enrollment/disenrollment information, if benefits are provided through one or more contracts of insurance HMOs/health insurance issuers is not required to provide a Notice of Privacy Practices.

**The Privacy Notice is provided by Florida Blue (the Group's Health Plan TPA) to the Group Health Plan participants (FCSRMC).**

# FCSRMC HIPAA Privacy Policy

**FCSRMC and it's member colleges have adopted a HIPAA Privacy Policy Statement. The Privacy Policy should be reviewed with new staff at the time of new hire orientation. Employees should sign the acknowledgement form indicating they have received and have had an opportunity to read the HIPAA Privacy Policy.**

# Consent and Authorization

Covered Entities cannot share PHI without the individual's awareness of their privacy rights.

To use and disclose PHI for purposes other than treatment, payment and health operation purposes, Covered Entities must obtain a standard consent or authorization with a few exceptions.

Consent can be revoked by an employee/individual (patient) when requested in writing, with few exceptions.

It is the policy of FCSRMC and its member colleges that individuals have a right to request that no disclosure be made of PHI.

# When Consent and Authorization IS Required

An authorization **is** required for:

- Use and disclose PHI for purposes other than treatment, payment and health operation purposes
- Marketing, research, sale of PHI, and fundraising
- Releasing PHI to the person's employer

**An authorization must include:**

- ❑ Description of the information to be disclosed
- ❑ Names of persons to whom the information is to be given
- ❑ Purpose of the disclosure
- ❑ An expiration date for the use of the information
- ❑ Individual's signature and date authorization was given

The authorization form for FCSRMC can be found on page 24 of the HIPAA Privacy Policies.

# When Consent and Authorization is NOT Required

- Treatment - Provision, coordination or management of healthcare and related services among healthcare providers or third party involved in healthcare operations
- Payment – Determining eligibility or coverage under a healthcare plan, adjudication of claims, billing/collection activities, utilization review activities
- Health Operations – Fraud/abuse detection, compliance programs, government inspections, competency assessments, business management activities
- Public health activities
- Law enforcement purposes
- To comply with Workers' Compensation
- To avoid serious threat to health or safety

# Court Orders and Subpoenas

A covered health care provider or health plan may disclose PHI required by a **court order**, including the order of an administrative tribunal. However, the provider or plan may only disclose the information specifically described in the order.

A **subpoena** issued by someone other than a judge, such as a court clerk or an attorney in a case, is different from a court order. A covered provider or plan may disclose information to a party issuing a subpoena if the employee has signed a HIPAA authorization form specifically releasing the information or if they receive evidence that reasonable efforts were made to either:

- Notify the person who is the subject of the information about the request so the person has a chance to object to the disclosure;

OR

- Seek a qualified protective order for the information from the court.

# Individual's Rights

Inspect and request a copy of medical record

Request restrictions on use/disclosure

Amend or update Information

Request accounting of all PHI disclosures

Obtain paper copy of Privacy Notice

Request confidential communications

File a complaint regarding privacy/security

***Requests for the above should be directed to, and processed by, Florida Blue (the Group's Health Plan TPA).***

# Individual's Rights

Staff can file a written complaint if they believe their privacy has been violated. Complaints should be directed to the college's privacy contact, and **any intimidating or retaliatory acts are prohibited.**

The Complaint Form can be found on page 26 of the Privacy Policies. Complaints should be documented on this form and forwarded to FCSRMC.

It is important for staff to know that their PHI is safeguarded to protect PHI from any intentional or unintentional use or disclosure that is in violation of the HIPAA Privacy Rule.

# "Minimum Necessary"

**"Minimum Necessary"** is limiting the amount of PHI that is used (within the facility) or disclosed (outside of the facility) to the least amount of information possible to accomplish the intended purpose.

- Your facility should evaluate **who** should be accessing PHI (documented in job descriptions).

- Only staff who need access to PHI to perform their job duties should be granted access to the software or files containing PHI and access should be controlled via a unique sign-on and password, key to locked doors/cabinets, etc.

Minimum Necessary does **not** apply to requests/disclosures to the staff or another healthcare provider for treatment purposes.

# Medical Information – Personnel Records

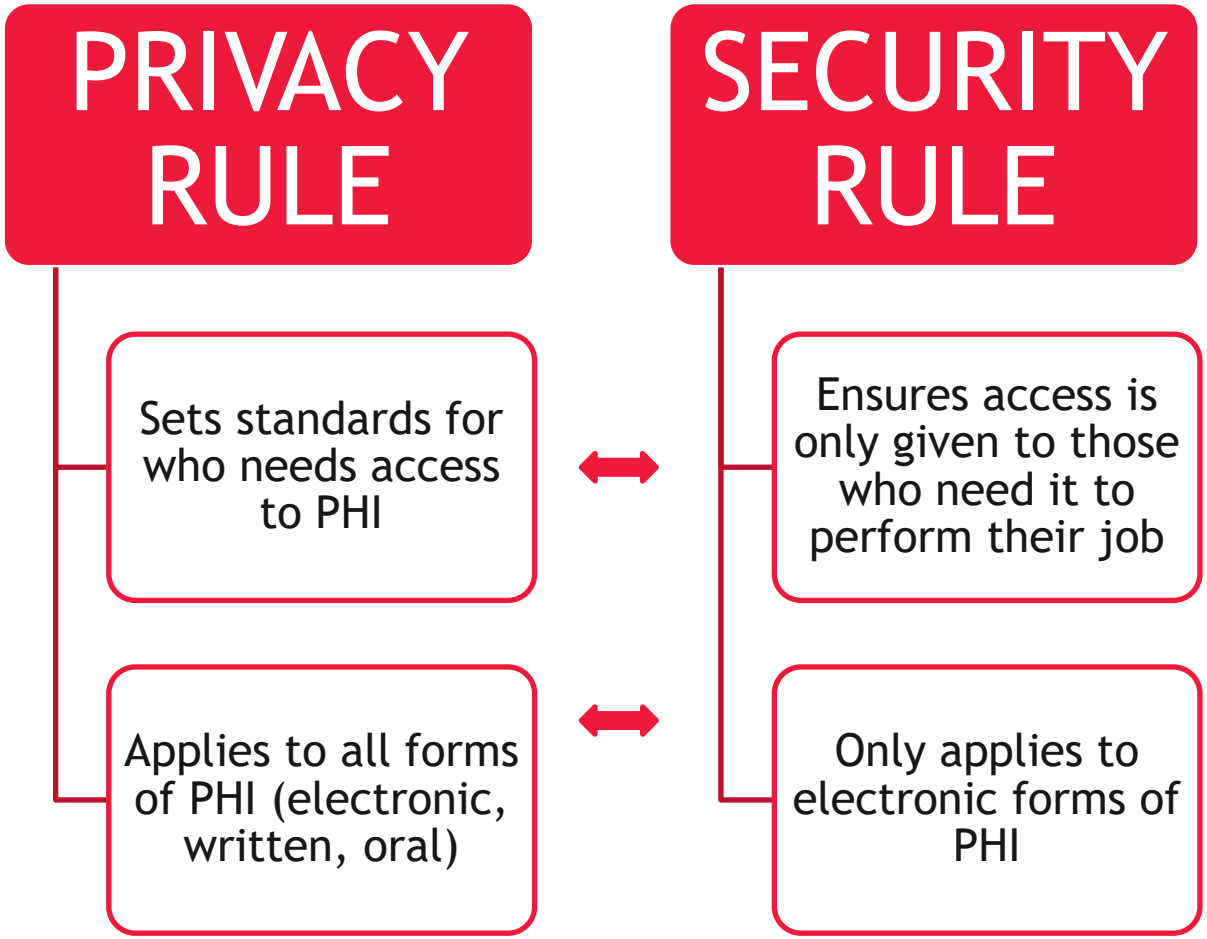
The Americans with Disabilities Act (ADA) and HIPAA require that **all medical documents be filed separately from personnel records**.

Medical information should be kept confidential and away from personnel records even if the company does not fall under ADA or HIPAA regulations.

Examples of medical paperwork that should be filed separately

- Reports from pre-employment physicals
- Drug and alcohol testing results
- Workers' compensation paperwork
- Medical leave of absence forms
- Disability paperwork
- Insurance applications
- Anything that identifies a medical issue

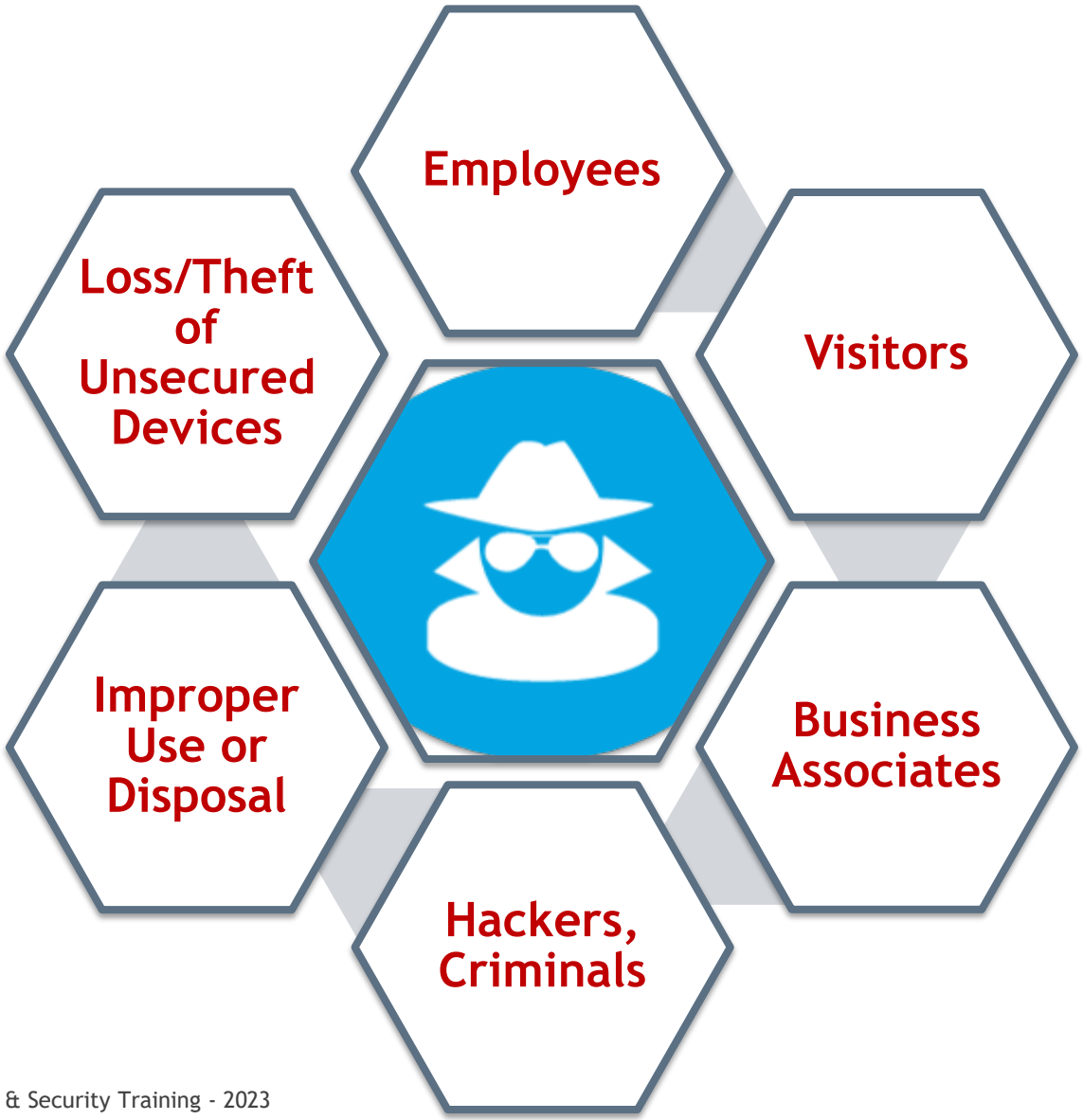
# HIPAA Privacy Vs. Security Rules



# HIPAA Security Rule

The Security rule addresses the measures organizations must take to protect information within their possession from both internal and external threats.

# Threats to Your PHI and Your Organization



# Administrative Safeguards

- Establish HIPAA policies/procedures and appoint a Privacy/Compliance Officer
- Provide security awareness training and periodically send reminders to staff
- Perform a risk analysis to determine where you might be vulnerable to a breach
- Have a Disaster Recovery Plan in place in case of an emergency
- Implement sanctions and terminations for staff who breach PHI
- Manage passwords, including disabling access upon termination
- Implement Business Associate Agreements for all vendors who access PHI

# Physical Safeguards

- Design a Continuity of Operations Plan when data is temporarily unavailable
- Implement a security plan for facility (door locks, video monitoring, etc.)
- Install password protection on monitors
- Ensure monitors are not facing public areas
- Password protect thumb drives and documents containing PHI
- Properly dispose of devices containing PHI (hard drives, copiers, fax machines)
- Ensure copiers and fax machines are not accessible by the public

# Technical Safeguards

- Only use certified software systems and install firewalls and antivirus software
- Use data encryption/decryption on all devices (laptops, cell phones)
- Back up data daily
- Assign unique sign-on and passwords to software containing PHI
- Utilize integrity controls to ensure PHI has not been tampered with or destroyed
- Implement automatic log-off after system has been idle
- Monitor/audit systems to ensure the system has not been hacked or compromised

# HIPAA Security Awareness

## Privacy Rule

- Providing patients with copies of their PHI upon request
- Obtaining authorizations when necessary
- Not disclosing more PHI than is necessay
- Prohibiting unauthorized disclosure of PHI on social media, email, text

## Security Rule

- Implementing safeguards to ensure confidentiality, integrity, and availability of PHI
- Implementing access controls to limit who can view PHI
- Executing Business Associate Agreements with vendors
- Guarding against unauthorized access of PHI

## Breach Notification Rule

- Notifying an impacted individual of a large security incident (500+ individuals)
- Notifying OCR of a large security incident within 60 days of discovery

# Staff Training

**Employers are required to provide privacy and security training to staff and to provide periodic security reminders.**

Security reminders may include:

- ✓ How to maintain security, including the need for strong passwords
- ✓ Specific threats to PHI that have been identified such as viruses
- ✓ PHI access restrictions
- ✓ Changes in policies/procedures concerning HIPAA regulations
- ✓ Procedures to follow for modifying access to PHI
- ✓ How to report security breaches and to whom

# Enforcement of HIPAA Compliance

**The Office of Civil Rights (OCR) enforces the Privacy and Security Rules in several ways:**

- Investigating complaints from individuals who believe their PHI has been compromised
- Conducting compliance reviews to determine if Covered Entities are in compliance
- Performing education and outreach to foster compliance with rules' requirements
- Making determinations regarding exceptions to state law pre-emption.

**Any person or organization can file a complaint with the OCR. Complaints typically must be filed within 180 days of the occurrence of an action that is in violation of the Privacy Rule.**

# Breach of PHI

A **breach** is any **unauthorized** access, use or disclosure of **unsecured** PHI which compromises the security or privacy of the PHI, unless there is a low probability that the PHI has been compromised.

Covered Entities and Business Associates must report a breach only if the breach involved unsecured PHI. Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified under the HIPAA guidelines.

If you feel a breach has occurred, an internal investigation should be conducted to determine if it is a reportable breach under provisions of the HIPAA Breach Notification Rule. The investigation should include:

- The nature and extent of the PHI involved
- The unauthorized person who used the PHI or to whom the disclosure was made
- Was the PHI actually acquired or viewed
- To what extent has the risk to PHI been mitigated

# Breach of PHI

There are three exceptions to the definition of “breach.”

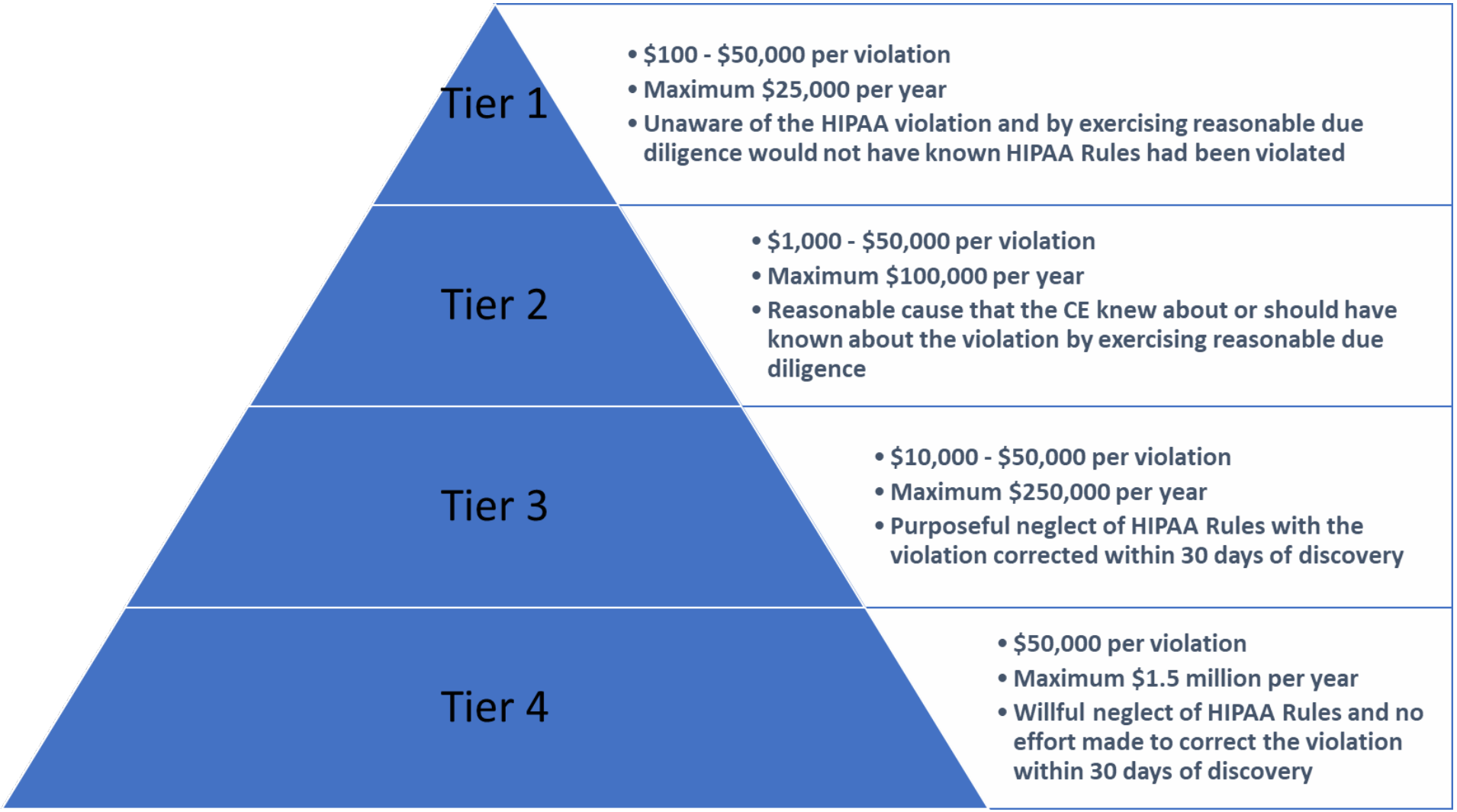
1. Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a Covered Entity or Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority.

2. Inadvertent disclosure of PHI by a person authorized to access PHI to another person authorized to access PHI at the Covered Entity or Business Associate.

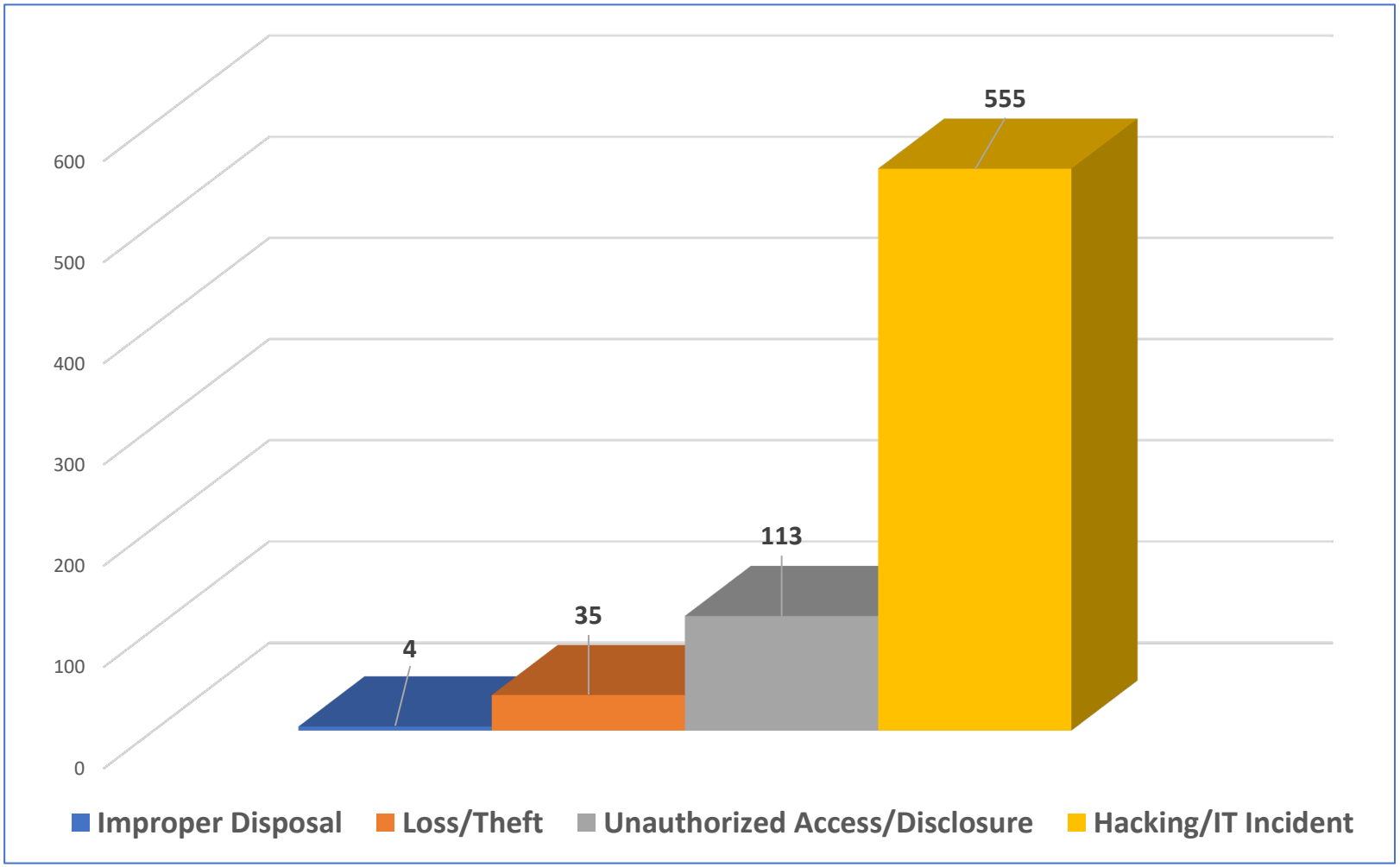
3. If the Covered Entity or Business Associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

Accidental HIPAA violations occur even when great care is taken by employees, and minor incidents can occur that are so inconsequential they do not warrant notifications to be issued.

# Penalties under HIPAA

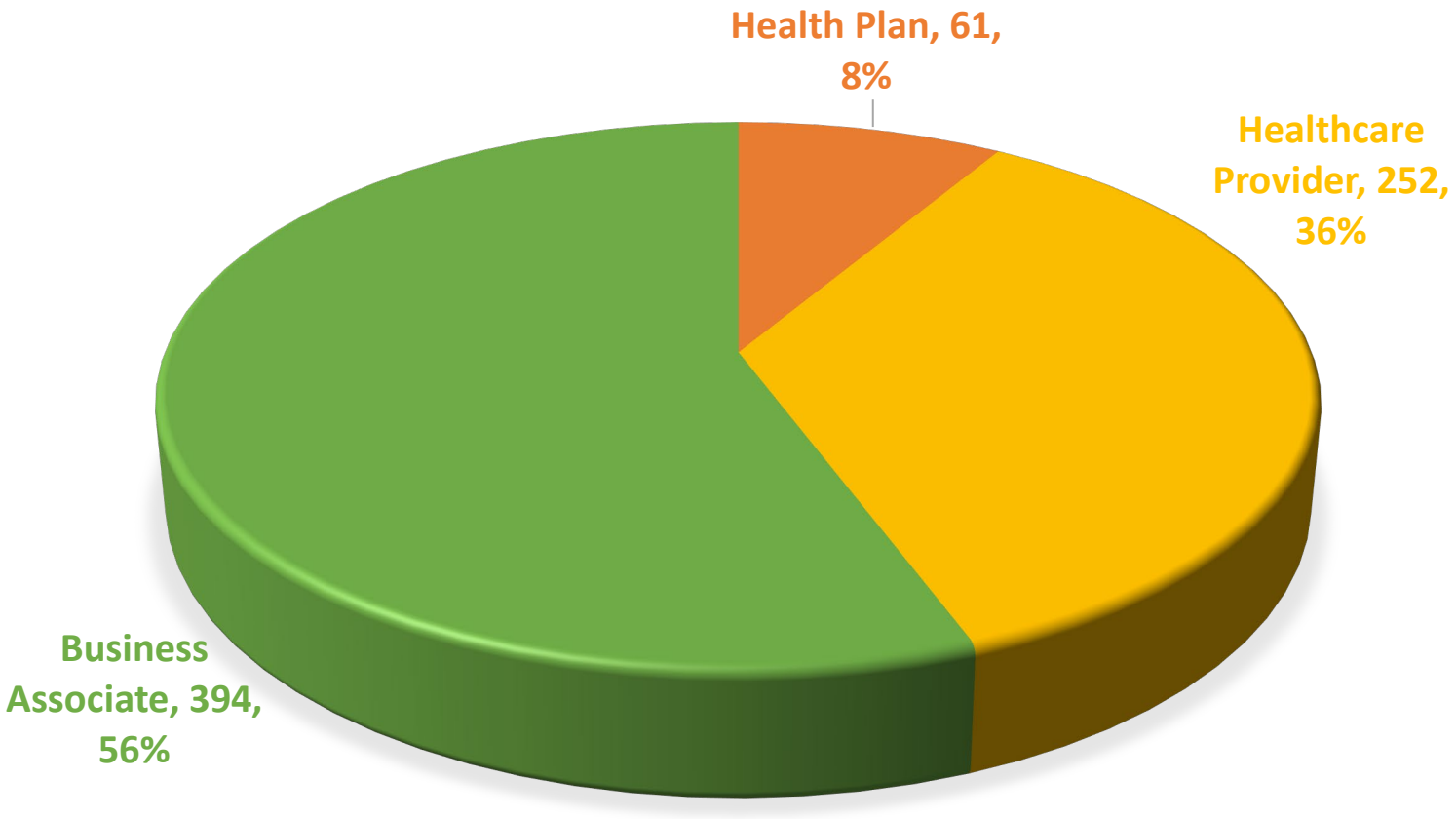


# HIPAA Data Breaches in 2022




Source: www.hipaajournal.com/healthcare-data-breach-statistics

# HIPAA Data Breaches in 2022




Source: www.hipaajournal.com/healthcare-data-breach-statistics

# Mitigating Risk

- ✓ Data protection
  - Use workstations properly - don't leave information open and unattended
  - Create strong passwords and don't share or post where others can see it
  - Don't discuss confidential information with unauthorized individuals
  - Lock computer, desk and file cabinets
  - Use shredder/recycle bin when destroying information
- ✓ Access controls – only give authorized staff access to software/files containing PHI
- ✓ Report potential threats to the Privacy Contact at your facility
- ✓ Encrypt emails containing PHI
- ✓ Obtain BAA from vendors when accessing/obtaining PHI
- ✓ Password protect mobile devices if accessing company emails on device
- ✓ Prevent malware infection on your computer by not downloading and installing anything you do not understand or trust, no matter how tempting
- ✓ Provide training at time of hire and annually thereafter

# Sanctions Policy

- All workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times.

- FCSRMC will take appropriate disciplinary action against employees, contractors, or any individuals who violate the information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- FCSRMC will impose sanctions on any individual who accesses, uses, or discloses sensitive information **without proper authorization**. Sanctions may include:
  - policy changes
  - personnel changes
  - transfer to another department
  - retraining
  - written reprimands
  - suspension
  - termination

# Documentation Retention

**Maintain the following documentation for six years, unless a longer period applies:**

- HIPAA Policies and Procedures
- Business Associate Agreements
- Signed Acknowledgement of Privacy Policies
- Authorization Forms
- Notice of Privacy Practices
- HIPAA Training Logs
- Complaints and their Disposition

# Quiz

1. Who is not a Covered Entity?
   a. Restaurant
   b. Physician
   c. Health Plan

2. Who must comply with HIPAA privacy and security rules?
   a. Only physicians and hospitals
   b. Patients
   c. All Covered Entities and Business Associates

3. Who should have access to PHI?
   a. Everyone in the company
   b. Everyone in the department
   c. Only those who need access to perform their job duties

4. It is OK to share your user-name and password with someone you know as long as they do not share it with anyone else.
   a. True
   b. False

Quiz

5. Who is considered a Business Associate?
   a. Janitor
   b. Postal Service
   c. I.T. Vendor

6. When is an authorization required to release PHI?
   a. When releasing information requested from an attorney
   b. When someone calls and asks for information about an employee
   c. Both a and b

7. How long is the document retention policy under HIPAA?
   a. 10 years
   b. 6 years
   c. Indefinitely

8. Ways to mitigate risk to PHI is:
   a. Secure your workstation and other areas containing PHI
   b. Don't report a breach if you suspect it has occurred
   c. Avoid the HIPAA training sessions

# References

**More detailed information can be found at the following resources:**

U.S. Department of Health and Human Resources. 45 CFR Parts 160 and 164. Federal Register
www.hhs.gov/ocr/privacy/hipaa/administrative/endorcementrule/enfifr.pdf

U.S. Department of Health and Human Services, Office for Civil Rights
www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf

Centers for Medicare & Medicaid Services, Office of E-Health Standards and Services.
www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliancerev08.pdf

U.S. Department of Health and Human Services.
www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule

Carol Crews, CMPE, CPMA, OHCC
Director, BDO Center for Healthcare Excellence & Innovation
ccrews@bdo.com
(904) 224-9787

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 650 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 80,000 people working out of 1,600 offices across 162 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.

www.bdo.com