

HIPAA Training January

"HIPAA 101"



HIPAA Rule Standards

KNOW THE RULES!

- The **Privacy Rule**, *protects the privacy* of individually identifiable health information;
- The **Security Rule**, *sets national standards* for the security of electronic Protected Health Information (ePHI).
- The **Breach Notification Rule**, *requires Covered Entities and Business Associates to provide notification following a breach* of unsecured Protected Health Information (PHI).

What is *Protected Health Information* (PHI)?



- Individually identifiable information.
 - Ex: name, address, SSN, birth date, etc. What can be used to identify the patient.
- If it relates to health care or health conditions of patient, it's PHI.
- Typically transmitted or maintained in electronic or other form or medium.

“Covered Entities,” *MUST* protect the privacy and security of PHI

Covered entities include:

- Health plans.
- Health clearinghouses.
- Health care providers who transmit health information in electronic form in connection with a "transaction" (e.g., claims submission).



Covered Entities: Business Associates



- Person who, on behalf of a covered entity, performs function/activity involving use or disclosure of PHI.
 - Examples:
 - claims processing,
 - accounting,
 - management,
 - administrative, or
 - legal services, copy service, etc.



When can PHI be disclosed?

- To the individual that the records pertain to.
- The facility/provider must permit the patient to view his or her records during business hours within five working days after receipt of the written request.
 - Paper copies to be provided within 15 days of request.
- For treatment, payment, or operations. (TPO).
 - Examples:
 - Doctor to doctor
 - Claims submission
 - Quality assessment
 - Improvement activities



PHI Disclosures (cont'd)

- With individual's permission
- By written request, to 3rd parties. (e.g., employer)
 - ***Note:** individuals can restrict what might otherwise be permitted disclosure to health plan, if they will pay for service out of pocket.
- De-identified information or PHI that has had enough personally identifiable information removed so that it can't be used to identify an individual.



Minimum Necessary “Need-to Know”

- Only those workforce members with a legitimate “*need to know*” may access, use or disclose PHI.
 - This includes, but is not limited to:
 - all activities related to Treatment, Payment and health care Operations (TPO).
- Each workforce member may *only access the minimum information necessary to perform his or her designated role* regardless of the extent of access provided to him or her.
- Just give what is needed to meet the purpose of the use or disclosure.
- *Limit access only to those people who need access to the information to accomplish the use or disclosure.*
- ***Do not give all information if they do not need/request all information.***

Minimum Necessary Principle does apply to (partial list):

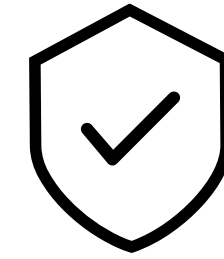
- Claims & billing
- Attorneys
- Insurance
- Disability
- Benchmarking reports
- Financial analysis
- Accreditation & licensure
- Credentialing
- Education and training
- Research



Minimum Necessary Principle does not apply to:

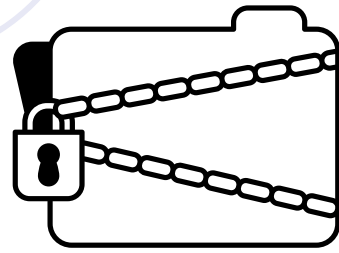
- Direct treatment situations in communications with other professional treating the patient.
- Disclosing medical information to the patient himself/herself.
- Disclosing information authorized for release by the patient.
- Certain disclosures required by law.

Security Rule Basics



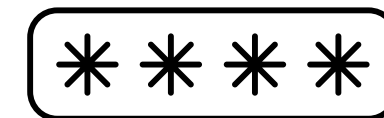
Applies to electronic PHI (EPHI) and Requires covered entities to maintain appropriate *administrative, physical, and technical safeguards*.

- **Administrative** - e.g., policies re: logging in & out, backing up data, etc.
- **Physical** - e.g., media controls (thumbdrives), access to server room, etc.
- **Technical** - e.g., having unique passwords for users, encryption, automatic logoff, etc.



Password Guidelines

- Users must select a password conforming to the following guidelines:
 - Passwords should be *between 8 and 10 characters*.
 - Passwords should NOT be the name of a pet, spouse, child, or parent.
 - Passwords should be a word or sequence of letters and numbers that the user can remember but could not be easily guessed by even a close friend of the user.
 - Passwords should NEVER be written down.
 - Should NEVER be given to other staff members.
 - A new password should be selected every 90 days, and current or previous passwords should NOT be re-used.



Security Rule Basics (cont'd)

- Requires thorough risk assessment (10 page checklist)
- Not one-size-fits-all. Take into account organization's finances, technical infrastructure, etc. Important thing is to have done risk assessment, and then actually follow through.



Breach Notification Rule Basics

- Relevant for unsecured PHI (UPHI) only.
 - "Unsecured" = not encrypted.
- Also only relevant when there has been a "breach."
 - "Breach" = non-permitted acquisition/access/use of UPHI that compromises security/privacy of information.
- All breaches should first be reported to:
 - Privacy Officer, Peachy Paulino
 - Email: compliance@prohealthpartners.com or
 - Fax: 562-299-5252.

"Breach" (cont'd)

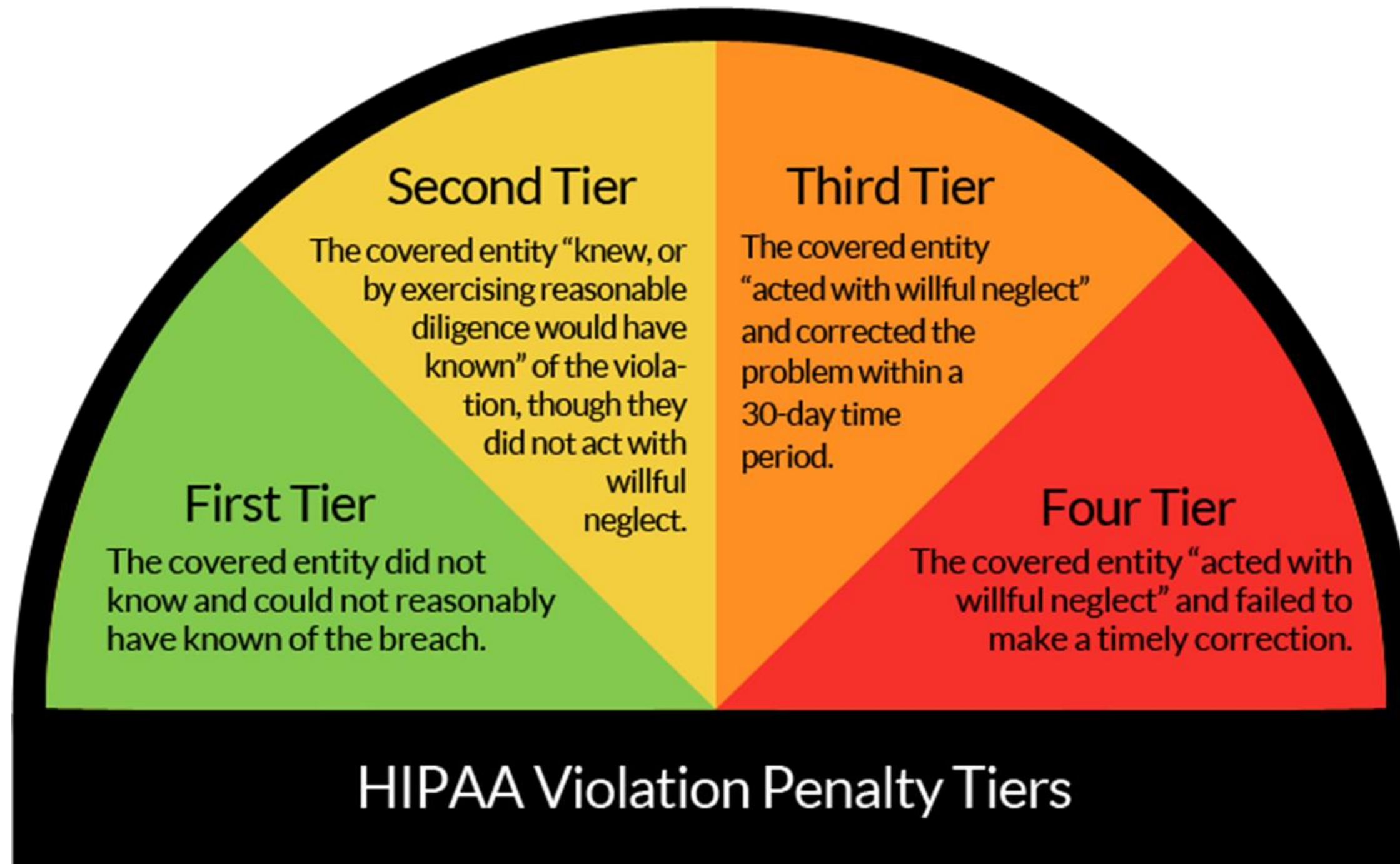
- To determine if breach has occurred, must examine risk factors (analysis of access to data):
 - Nature and extent of PHI involved, including ability to re-identify.
 - Unauthorized person to whom disclosure was made or who used the PHI.
 - Whether PHI was actually acquired or viewed.
 - Extent to which risk to PHI has been mitigated.
 - Ex: Accidental fax to wrong physician's office, with recipient destroying fax. No breach, no notification required.
 - Ex: Lost laptop/thumb-drive, probable breach, notification required.

Breach Notification Rule Requirements

Notification must be made:

- **To the individual.**
- **To Secretary of HHS** In cases of 500+ breaches.
 - Also in cases of less than 500 breaches, within 60 days of the end of the current calendar year.
- **To media** in cases of 500+ breaches.

Civil Penalties



HIPAA CRIMINAL PENALTIES

- Covered entities or individuals who knowingly or with reasonable cause obtain or disclose individually identifiable health information:
 - Penalty: Up to one-year potential jail sentence + up to \$50,000 fine
- Offenses committed under false pretenses:
 - Penalty: Up to five years potential jail sentence + \$100,000 fine
- Offences committed with intent to sell, transfer, or use for personal gain or malicious reasons:
 - Penalty: Up to ten years potential jail sentence + \$250,000 fine
- No criminal penalty for “Unknowingly”.
- Office of Civil Rights (OCR) Website: for resources:
 - <http://www.hhs.gov/ocr/office/index.html>



VERY IMPORTANT!!!

- Fill out Form Compliance Attestation Form, found on ArgusLink.
- ***This is a requirement for HIPAA Compliance!***
- Where to Keep the Form?
 - Keep Original Copy in the Employee Personnel File.
 - Email copy to:
 - compliance@prohealthpartners.com



2025 Compliance Trainings Attestations

I attest that:

I have completed the required training for the following: (Submit form only when all trainings are complete).

>> mark boxes below of topics completed.

- Health Insurance Portability and Accountability Act (HIPAA)
- Occupational Safety and Health Administration (OSHA)
- Fraud, Waste, and Abuse (FWA)
- Cultural and Linguistic Competency
- Code of Conduct
- Disability & Discrimination

Note: Worksite Hazard and C.U.R.E.S attestations are separate forms.

- I listened, read, and understood the course and information as presented. As an employee, I understand that it is my responsibility to abide by ProHealth Partners, A Medical Group/Argus Medical Management policies and procedures, in accordance with the training.
- The trainings were downloaded from ArgusLink Operations page and presented without modification in accordance to ProHealth Partners, A Medical Group/Argus Medical Management Policies and Procedures.
- AND/OR I completed the above listed training through another source in this year and have corresponding documents.
- If I have questions about the training, materials presented or ProHealth Partners, A Medical Group/Argus Medical Management policies and procedures, I understand it is my responsibility to seek clarification from the Compliance Officer or Human Resources Department.

Doctor Office Name/ Location _____

Print name _____

Employee or Doctor Signature _____

Date _____

Email completed form to
compliance@prohealthpartners.com
or Fax (562) 299-5273

DEADLINE 12/31

