



What Employers Should Know About HIPAA



Erin DeBartelo,
PHR, SHRM-CP
Principal Hotline Advisor



Laura Kerekes,
SPHR, SHRM-SCP
Chief Knowledge Officer



- This session is being recorded.
- Download the slides and handouts on the handouts widget.
- You will receive a link to the recording after the webinar.
- We will provide the HRCI and SHRM codes at the end of the webinar.
- Ask questions using the question box. Our hotline team will answer your questions within the next few days.

1

HIPAA
Definitions
and Coverage

2

Privacy and
Security Rules

3

Managing HIPAA
Requirements

4

ThinkHR
Support and
HRCI/SHRM
Codes

1

HIPAA Definitions

Health Insurance Portability and Accountability Act of 1996 (HIPAA)





HIPAA Coverage

Applies to covered entities and business associates

Covered entities include:

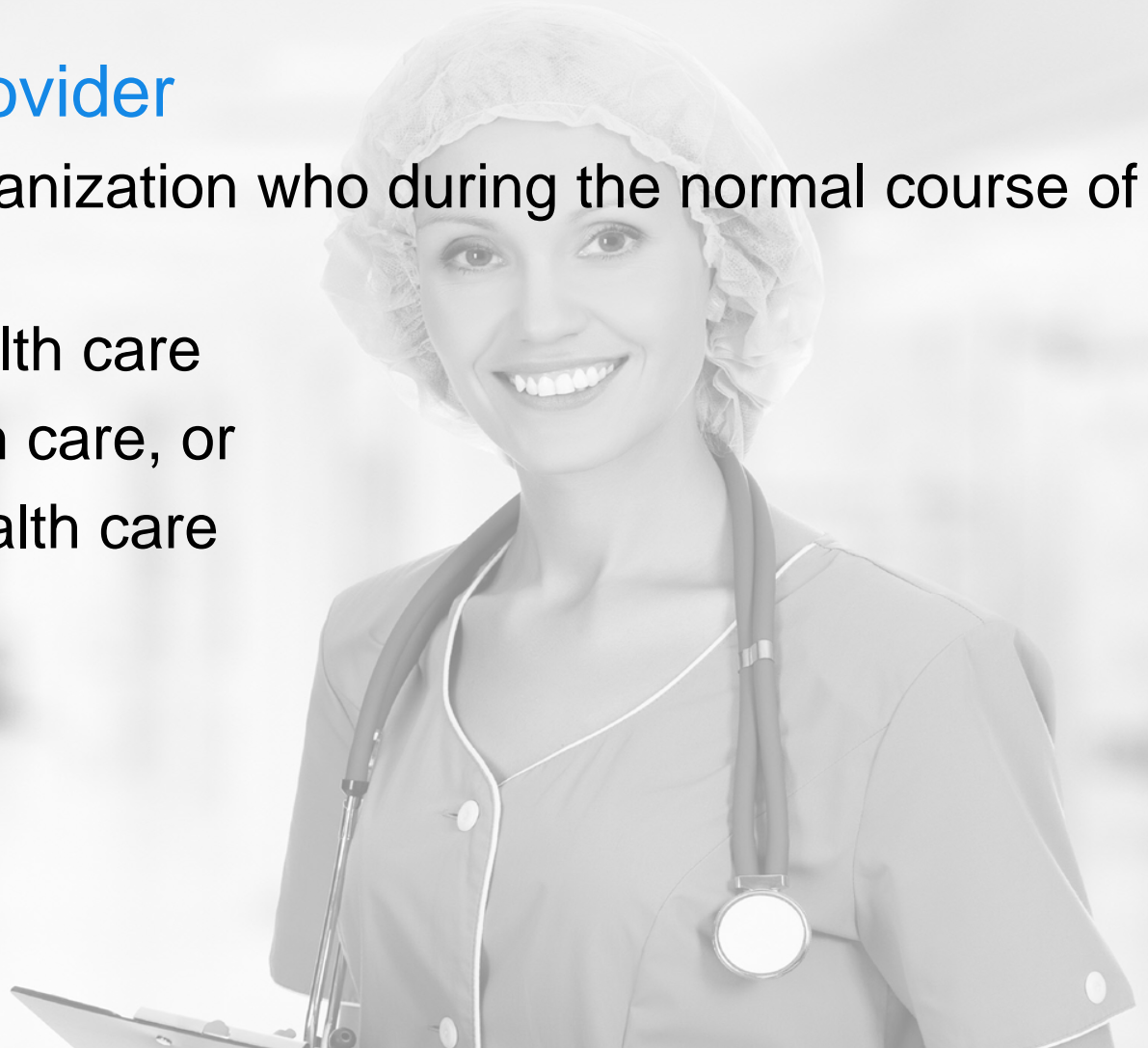
- “Covered health care providers” (electronic transactions)
- Health care clearinghouses
- Health plans

HIPAA Coverage

Health Care Provider

Any person or organization who during the normal course of business:

- furnishes health care
- bills for health care, or
- is paid for health care



HIPAA Coverage

Health Care Clearinghouse

Processes health information data content/format for another entity from non-standard to standard or vice versa.

HIPAA Coverage

Group Health Plan

Any individual, group plan, or combination that provides or pays for the cost of medical care

Examples:

- Health insurance issuers
- HMOs
- Group Health Plans
- Medicare, Parts A and B
- Medicare + Choice
- Medicaid

HIPAA Coverage

All health plans are covered

Entities not considered health plans:

- Excepted benefit plans
- Certain government funded programs

HIPAA Coverage

Exempt organizations include most:

- Schools and school districts
- State and municipal agencies and offices
- Law enforcement agencies
- Workers' compensation and life insurance carriers
- Employers with fully insured group health plans that obtain doctors' notes to administer sick leave, wellness plans or workers' compensation.

HIPAA Coverage



HIPAA Coverage

And:

Employers sponsoring self-funded (self-insured) HIPAA-covered group health plans **ARE SUBJECT** to HIPAA

HIPAA Coverage

Business Associates

Contractors, subcontractors and other outside persons or companies with access to personal health information when providing services

- Billing and claims processing companies
- Companies storing/destroying medical records
- Health plan administration companies
- Outside legal, financial or technical experts

2

Privacy and Security Rules

Privacy Rule

Goals of the Privacy Rule

- Protect individual health information while allowing that information to be shared between providers to promote quality health care and public safety
- Set limits for who can obtain that health information in all formats (oral, paper, electronic)
- Enable individuals to know how that protected personal information has been disclosed
- Gives patients the right to examine their health records and request corrections

Privacy Rule

Health Plan Requirements

- Notify participants of their rights and how their information can be used
- Adopt privacy procedures
- Train employees on privacy rules
- Designate a privacy officer or someone to oversee these privacy rules and procedures
- Adopt systems and processes to secure PHI

Privacy Rule

PHI includes:

- Past, present or future physical or mental health condition
- Description of health care provided
- Past, present, or future payment for health care provided that either identifies the individual or reasonably could be used to identify the individual
- Individually identifiable health information with common identifiers (e.g., name, address, birth date, Social Security Number)

Security Rule



Security Rule

Goals of the Security Rule

- Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity
- Requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information

Security Rule

Who is covered by the Security Rule?

Health Plans, Health Care Clearinghouses, and any Health Care Provider who transmits health information in electronic form

What information is protected?

Electronic Protected Health Information: PHI in electronic form (not PHI transmitted orally or in writing)

Security Rule

Safeguards for e-PHI

- Ensure confidentiality, integrity, and availability of all e-PHI created, received, maintained or transmitted;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by company employees

Security Rule

Covered entities should consider the following:

- Organization size, complexity, and capabilities
- Technical, hardware, and software infrastructure
- Cost
- Likelihood and possible impact of potential risks to e-PHI

3

Managing HIPAA requirements

Employer Role in Managing HIPAA

Reminders and Cautions

- While HIPAA may not apply because you collect some employee health information, HIPAA affects you in the process of getting the information from covered health care providers
- Important as you collect information for FMLA or ADA reasons (need valid patient authorization for disclosure of PHI)
- Generally not so under Workers' Compensation, but check state rules

Employer Role in Managing HIPAA

For employers with self-funded group health plans, establish your HIPAA privacy and security plans

- Limit access to PHI—only to employees who perform plan administration functions
- Train these employees to understand obligations for the Privacy Rule
- Implement the physical, technical and administrative safeguards in the Security Rule for electronic PHI

Employer Role in Managing HIPAA

For employers with self-funded group health plans, establish your HIPAA privacy and security plans

- Notify plan participants when a security breach occurs
- Don't disclose PHI to "business associates" until they sign the BA agreement
- Notify employees of your privacy practices
- Establish your policies and procedures to administer HIPAA rules
- Make sure your plan documents reflect the HIPAA rules

Final Thoughts

Ensure that:

1. You have a HIPAA privacy policy in your employee handbook.
2. Any staff who may come in contact with benefits-related information are trained on the basics of HIPAA privacy. Document that training was completed.
3. All enrollment forms, bills and anything related to GHP is maintained in a locked private area. Be sure any electronic information is password protected and not available on a company-wide intranet or access point.
4. You have a Business Associate Contract with any person or vendor your company does business with who may come into contact with benefit-related information

4

ThinkHR Support

Accessing Your ThinkHR Resources

Sign in

Thinkhr.com or your broker's custom URL

Contact the ThinkHR Live team

877-225-1101 or via Workplace