Privacy of Employee Medical Information

Sheba Vine, Esq., CIPP/US
VP, General Counsel
First Healthcare Compliance, LLC

Objectives

- When HIPAA Applies
- Requesting Medical Information
- Federal and State Laws that Protect Employee Medical Information
- Putting Policies in Place

When HIPAA Applies

HIPAA Basics

The **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct

- Federal law, enacted in 1996
- Administrative simplification provisions focus on improving efficiency of healthcare delivery through standards and electronic transmission of health information
  - Privacy Rule –standards for protecting health information
  - Security Rule – standards for protecting electronic health information

(45 CFR Part 164 et seq.)

When HIPAA Applies

Covered Entities (CE)

Business Associates (BA)

If an employer does not meet the definition of a CE or BA it does not have to comply with HIPAA

Covered Entities

Healthcare Providers

- Provides, bills or is paid for health services if it transmits health information in electronic form (doctors, hospitals, long-term care facilities, home health agencies)

Health Plan

- Individual or group plan that pays for treatment or care (health insurance companies, HMOs, employer sponsored group health plans)

Healthcare Clearinghouse

- Translates healthcare transactions from non-standard to standard format and vice versa (billing services, re-pricing companies, community health management information systems)

Business Associates

- Not a member of a Covered Entity's workforce
- Assists Covered Entity in performing functions that involve creating, receiving, maintaining or transmitting Protected Health Information (PHI):

  - Claims processing
  - Data analysis
  - Utilization review
  - Billing
  - Legal
  - Actuarial
  - Accounting
  - Consulting
  - data aggregation
  - Management
  - Administrative
  - Accreditation
  - Financial services

Information Protected by HIPAA

Protected Health Information (PHI):

- information created or received by a health care organization
  - Relates to an individual's past, present or future health or condition
  - Provision of healthcare to an individual; or
  - Past, present, or future payment for the provision of healthcare to an individual
- When coupled with data that can potentially identify the patient

HIPAA Identifiers

- Name
- Addresses
- Telephone number
- Fax number
- Email address
- Social security no.
- Medical record no.
- Certification/license no.
- Vehicle identifiers/serial no.
- Device identifiers/serial no.
- IP addresses
- URLs
- Biometric identifier (fingerprint/voiceprint)
- Full-face photographic image
- Date of birth, death
- Date of admittance, discharge
- Account numbers
- Health plan beneficiary no.
- Other unique identifying no., characteristics or codes

Exceptions

- HIPAA does not apply to the following records that contain health information (even if employer is a Covered Entity):
  - Employment records (sick leave requests, FMLA/ ADA-related information, drug test results)
  - Education records covered by Family Educational Rights and Privacy Act (FERPA)
  - PHI of individual that has been deceased for more than 50 years
  - De-identified PHI

45 CFR § 160.103

Impact on Employers

HIPAA impacts an employer's request for health information from a health care provider

- HIPAA Authorization is needed before the provider discloses any health information
  - unless information is for payment, treatment, healthcare operations or public policy reasons
- Impacts employer when handling FMLA, ADA, etc. for employees that requires health information

Requesting Medical Information

HIPAA Authorization

- As a general rule, health care providers will require a written authorization signed by the employee/patient before disclosing medical information directly to the employer

- To avoid this, employer can request the medical information directly from the employee, rather than from the health care provider, if practical.

HIPAA Authorization Cont.

- Valid authorization includes the following:
  - Description of the information requested and purpose of disclosure
  - Name of the employer authorized to receive the PHI
  - Expiration date
  - Signature and date of the employee authorizing the disclosure
  - Statement regarding
    - employee's right to revoke and the process for revoking the authorization
    - information disclosed may be redisclosed, and may no longer be protected
    - prohibition against withholding treatment, payment, enrollment, or eligibility for benefits for refusing to sign

Family and Medical Leave Act (FMLA)

- Eligible employees permitted 12 weeks of unpaid, job-protected leave for serious health conditions or to care for a family member with a serious health condition
  - 50 or more employees/ work 1250 hours in 12 months
- Employer may require a medical certification from a health care provider to support the need for FMLA leave
  - If employee is responsible for returning completed certification to employer → no authorization
  - If healthcare provider is responsible for returning completed certification to employer → HIPAA authorization

FMLA – Authentication v. Clarification

Authentication: To verify that the information is complete and/or authorized by the health care provider who signed the document

- Authorization not needed as long as content of certification is not discussed

Clarification: To understand the handwriting on the medical certification or to understand the meaning of a response

- HIPAA Authorization
- Cannot require authorization. If employee chooses not to provide authentication and does not otherwise clarify the certification then FMLA leave can be denied.

Only HR professional, leave administrator or management official is allowed to contact provider-- not the direct supervisor

Americans with Disabilities Act (ADA)

- Prohibits discrimination against employees with disabilities. Qualified employees are entitled to reasonable accommodations
  - 15 or more employees
- In determining whether a reasonable accommodation exists the employer may request medical documentation of a disability
- If provider sends the documentation directly to employer or if employer needs to contact health care provider → HIPAA authorization

Drug Testing

- HIPAA authorization needed before releasing exam results to the employer

Federal and State Laws that Protect Medical Information

Confidentiality

- No single source of the right to privacy
- Laws that require confidentiality:
  - FMLA
  - ADA
  - GINA
  - EEOC
  - OSHA
  - State laws

Confidentiality: FMLA, ADA and GINA

- Medical information must be treated as confidential and kept separate from the employee's personnel file
  - FMLA related information of employees and their family members *(29 CFR § 825.500)*
  - ADA/disability related information for job applicants and employees *(29 C.F.R. § 1630.14(c))*
  - Genetic information obtained under GINA's limited exceptions *(29 C.F.R § 1635.9)*

Confidentiality Exceptions: FMLA

- Medical information can be disclosed in limited situations:
  - Supervisors and managers who need to know about necessary restrictions on work duties and accommodations.
  - First aid and safety personnel, if the employee's condition might require emergency treatment.
  - Government officials investigating compliance with the FMLA (or other pertinent laws)

Confidentiality Exceptions: ADA

- Medical information can be disclosed in limited situations:
  - Supervisors and managers who need to know about necessary work restrictions or accommodations;
  - First aid and safety personnel, if a disability might require emergency treatment;
  - Government officials investigating compliance with the ADA; and
  - When required for workers' compensation laws or for insurance purposes (from EEOC guidance)

- According to EEOC 'keep medical information in a separate medical file that is accessible only to designated officials. Medical information stored electronically must be similarly protected.''

Holtrey v. Collier County Board of Commissioners

- Employee took FMLA leave for a medical condition involving his genitourinary system
- During a staff meeting, a manager openly discussed employee's medical condition to co-workers (no consent, no reason to disclose)
- Employee was harassed by co-workers, including obscene gestures and inappropriate jokes.
- Employee filed a lawsuit claiming interference and retaliation under FMLA.

Employer's disclosure of medical information violated FMLA's confidentiality provisions

Confidentiality: EEOC

- Drug test results that reveal the presence of a lawfully prescribed drug or other medical information must be treated as confidential.
    - Results should be filed separate from the employee personnel file

Confidentiality: Occupational Safety and Health Administration Act (OSHA)

- To protect privacy, employee's name is not included for following injury or illness on OSHA 300 Log
  - To intimate body part or the reproductive system
  - resulting from a sexual assault
  - Mental illnesses
  - HIV infection, hepatitis, or tuberculosis;
  - Needlestick injuries and cuts contaminated with another person's blood or other potentially infectious material
  - Other illnesses, if the employee voluntarily requests that his or her name not be entered on the log.
- Employer may use discretion in describing the injury or illness
- Must keep a separate, confidential list of the case numbers and employee names for government investigation purposes.

29 C.F.R. §1904.29(b)(6)-(b)(7)

Sec'y of Labor v. United States Postal Service

- Employee's FMLA leave application included statement from doctor that she had a "serious health condition…caused by her work environment exclusively."
- $5,000 OSHA citation for not recording occupational illness on OSHA forms.
- Appealed ALJ's decision; Occupational Safety & Health Review Commission held that the confidentiality provisions of FMLA supersede OSHA's recordkeeping requirements.

Carefully evaluate handling of employee information and comply with various confidentiality requirements.

Delaware Law on Destruction of Employment Records

Delaware requires personal identifying information to be destroyed by rendering it unreadable or indecipherable (e.g., shredding, erasing).

Personal identifying information defined as employee's first name or first initial and last name with one of the following (if unencrypted):

- **confidential health care information**
- Social Security number
- driver's license
- state identification card no.
- insurance policy no.
- financial services account no.
- bank account no.
- credit card no.
- debit card no.
- tax or payroll information
- passport no.

Del. Code 19 § 736

New Jersey Earned Sick Leave Law

- Effective 10/29/18
- Allows employee to accrue 1 hour of earned sick leave for every 30 hours worked, up to 40 hours each year
- Employer may request documentation from healthcare provider for certain unforeseeable leave or if 3 or more consecutive days are taken
  - Must be kept confidential
- Private right of action

N.J.S.A. § 34:11D-1 et seq.

Connecticut Personnel Files Act

- Act requires employers to maintain personnel and medical records separately.

Conn. Gen. Stat. § 31-128c

Virginia's Limitation on Re-Disclosure

- Law limits an employer's re-disclosure of patient health information received
- Disclosure requires authorization from the employee

> *"no person to whom health records are disclosed shall redisclose or otherwise reveal the health records of an individual, beyond the purpose for which such disclosure was made, without first obtaining the individual's specific authorization to such redisclosure…"*

Virginia Code § 32.1-127.1:03

Breach Notification Laws

- Every state has its own version- definition of personal information, notice requirements, exceptions
- Applies to electronic consumer information, including employee information
- Breach causes reputational damage, cost of legal defense, dealing with regulators, and potential for lawsuits
- Focus on prevention- safeguard employee information

Breach Notification- Delaware

- Notify affected individuals of a data breach within 60 days
- Notify state AG if breach > 500 residents
- Offer free credit monitoring services for 1 year if breach includes Social Security no.

Del. Code 6, § § 12B-101

First name/ initial	Last name
Medical history, treatment or diagnosis by a health care professional, or DNA profile	Driver's license/state or federal identification no.
Health insurance id. no.	Social Security number
Passport number	Account number
Individual taxpayer id no.	Biometric data
Username/email with a password/security question and answer that would permit access to an online account	Credit/debit card no. with security code/ password

Breach Notification- Connecticut

- Notify affected individuals without unreasonable delay, no later than 90 days
- Notify State AG
- Offer identity theft protection services at no cost to residents for at least 24 months if social security numbers compromised

First name/ initial and last name
Social Security no.
Driver's license no. or a state id no.
Account no or credit/debit card no. with security code or password

Conn. Gen. Stat. § 36a-701b

Breach Notification- New York

- Notify affected individuals without unreasonable delay
- Notify State AG, department of state and the division of state police
- Notify consumer reporting agencies if breach > 5,000 residents

Any personal information combined with:
Social Security no.
Driver's license no. or a state id no.
Account no or credit/debit card no. with security code or password

N.Y. Gen. Bus. Law § 899-aa

Breach Notification- Pennsylvania

- Notify residents of breach of computerized data without unreasonable delay
- Notify nationwide consumer reporting agencies if breach > 1,000 individuals

First name/ initial and last name
Social Security no.
Driver's license no. or a state id no.
Financial account no. or credit/debit card no. with security code or password

73 Pa. Stat. § § 2301 et seq.

Breach Notification- Virginia

- Notify residents and state AG of breach without unreasonable delay
- Notify nationwide consumer reporting agencies if breach > 1,000 individuals

First name/ initial and last name
Social Security no.
Driver's license no. or a state id no.
Financial account no. or credit/debit card no. with security code or password
Passport no.
Military ID no.

Va. Code § 18.2-186.6

Dittman v. University of Pittsburgh Medical Center

- 2014 data breach of network resulted in theft of personal information of 62,000 employees
  - Social Security no., birthdates, tax information, addresses, salaries, and bank account info. that led to fraudulent tax returns
  - Class action alleging that UPMC breached a common law duty of reasonable care to secure their personal information, which they provided as a condition of their employment
  - Lacked adequate security measures (firewalls, encryption, authentication)
- Pennsylvania Supreme Court held that employers have a common law duty to use reasonable care to protect sensitive personal information held electronically

Takeaway: Employers must provide adequate privacy protection measures for employee data

2018 Pa. LEXIS 6051 (Pa. Nov. 21, 2018)

Putting Policies in Place

Steps to Take

- Prepare a template HIPAA Authorization form for employees to sign prior to requesting medical information from health care providers
- Review employee forms and eliminate requests for unnecessary personal information.
- Establish policy on maintaining medical information in separate confidential files.

Medical exams /certifications	Medical information about an employee's family members
Drug/alcohol tests	Workplace injuries/illness
Worker's compensation claims	Requests for leave of absence
FMLA leave paperwork	Doctor’s notes
ADA accommodations paperwork	Fitness for duty certification/exam

Steps to Take

- Maintain paper and electronic records securely and limit access to the appropriate individuals.
- “clean desk” policy- require employees to secure sensitive paperwork when they leave at the end of the day.
- Train employees/supervisors on the importance of maintaining confidentiality, and about the limits on disclosure of confidential information.
- Address confidentiality/ security in vendor contracts if disclosing employee information.
- Implement a document destruction policy.
- Implement breach response plan for unauthorized disclosure of employee information.
- Conduct an audit of policies
- Monitor state and federal law regarding confidentiality

Sheba Vine, Esq., CIPP/US

Vice President, General Counsel

First Healthcare Compliance, LLC

shebavine@1sthcc.com

www.1sthcc.com