Fall 2021

Office of General Counsel

Basic HIPAA Overview

Daniel McCabe
Assistant General Counsel

Presentation Content

- Part One: What is HIPAA?
- Part Two: HIPAA Compliance Steps
- Part Three: HIPAA Practical Scenarios

First – A Note

- This presentation is a general overview of HIPAA. It supplements, but does not replace, annual HIPAA training for employees who work with Protected Health Information as defined by HIPAA.

Part One: What is HIPAA?

HIPAA Background

- Health Insurance Portability and Accountability Act of 1996
- National standards for electronic health records and security
- Subsequently expanded by the Health Information Technology for Economic and Clinical Health Act (HITECH Act)

The Privacy Rule

- The Privacy Rule sets national standards for the protection of “Protected Health Information” (PHI).
- It applies to:
  - Covered Entities (Health Plans, Healthcare Providers, Healthcare Clearinghouses)
  - Healthcare components of Hybrid Entities
  - Business Associates

What is PHI?

- PHI is information, including demographic data, that relates to:
  - An individual's past, present or future physical or mental health or condition,
  - The provision of health care to an individual, or
  - The past, present, or future payment for the provision of health care to an individual.
- PHI either identifies an individual or there is a reasonable basis to believe it can be used to identify an individual.

What is a Covered Entity?

- Health Care Plans: Insurance Companies, HMO's, Medicare, Medicaid, etc.
- Health Care Providers: Doctors, Dentists, Hospitals, Pharmacies, etc.
- Health Care Clearinghouses: Billing processors

What is a Hybrid Entity

- The Minnesota State Colleges and Universities are a “Hybrid Entity.” This means that we provide some healthcare services.
- Our so-called “healthcare components” provide “covered functions.”

What is a Covered Function

- Provides health care services to non-students.
- Bills those patients' insurance for those services.
- Does so electronically.

Student Health Centers

- Student Health Centers are usually not healthcare components.
- Exceptions include if the health center treats students after graduation, treats employees, or treats students of non-Minnesota State colleges or universities AND bills those patients' insurance electronically.

Our Healthcare Components

- The Dental Hygienic Clinic, Speech and Language Therapy Clinic, and Student Health Services at Minnesota State University – Mankato
- The Dental Hygienic Clinic at Minnesota State Community and Technical College
- The Dental Hygienic Clinic at Rochester Community and Technical College.
- Administrative personnel and offices within Minnesota State, to the extent they perform support functions on behalf of any of the Health Care Components listed above.

Business Associate Agreements

- Business Associates provide services to covered entities.
- Unless a transaction involves one of our healthcare components, we do not need to enter into Business Associate agreements.

The Security Rule

- The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

Breach Reporting

- Just like the Minnesota Government Data Practices Act, there are Data Breach notification and remediation requirements.
- If a Healthcare Component suspects a data breach involving PHI, notify OGC and System Office IT Security Immediately.

HIPAA and FERPA

- Student health data is not governed by HIPAA. It is governed by FERPA.
- Joint federal Dept. of Education and Dept. Health & Human Services guidance.
- Student health providers can keep “Treatment Records” to themselves similar to the “Sole Possession Record” rule under FERPA.

Medical Data Rule under MGDPA

- Even if your clinic is not governed by HIPAA, you still may have private data under the MGDPA.
- If you provide free services or do not bill patient insurance electronically, but treat non-students, their data is Private Medical Data under the MGDPA.

Part Two: Compliance Checklist

MINNESOTA STATE
18

Is it a Health Care Component?

- Does it provide medical services (dental hygiene, nursing, physical therapy, speech therapy, pharmacy, etc.)?
- Does it treat non-student patients?
- Will it bill patient insurance electronically?

Privacy Officer

- Your campus needs an individual designated as a HIPAA Privacy Officer.
- This individual is ultimately responsible for your HIPAA compliance.

Complaints

- Your campus needs someone to whom patients can direct HIPAA related complaints.
- This can be the same person as the Privacy Officer.
- You also need a process for accepting and addressing complaints.

Safeguards

- Your campus needs appropriate, Security Rule compliant safeguards to protect PHI.
- Consult System Office IT for electronic records.
- For hard files, maintain them as you do private data protected by the MDGPA/FERPA.

Mitigation and Resolution of Issues

- Process to sanction employees for HIPAA violations
- Process to mitigate damage caused by HIPAA violations (including statutorily mandated notification and remediation)

HIPAA Privacy Policy and Patient Notification

- To be HIPAA compliant, you need a HIPAA privacy policy, and you need to inform patients of this policy.
- There are already such policies in our System, you do not have to draft a new one.

Part Three: Practical Scenarios

Practical Scenarios - Students

- You heard that student vaccine records are governed by HIPAA, so you keep them as private data. Are they covered by HIPAA? If not, are they private data?
- A student asks for a HIPAA privacy policy related to their disability services records, what should you do?
- Your student health center treats students who have graduated in the last year. Does it have to be HIPAA compliant now?

Practical Scenarios – Students (Answers)

- Student vaccine records are private data under FERPA, not HIPAA.
- Disability services records are governed by FERPA. You may refer the student to the annual notice of FERPA rights.
- If student health centers treat alumni AND bill those alumni's insurance electronically, they are performing a covered function under HIPAA.

Practical Scenarios – Healthcare Components

- Your dental clinic sees patients from the general public. It provides a free service. Does your clinic have PHI?
- Your athletic trainer has been billing patients electronically, but only sees student patients. Do they have PHI?
- Your speech therapy clinic bills patient insurance electronically, and treats non-students. Does it have PHI?

Practical Scenarios – Healthcare Components (Answers)

- Clinics that provide only free services do not have PHI.
- College/University employees and contractors who only treat students do not have PHI.
- Operations that treat non-students and bill their insurance electronically HAVE PHI.

Practical Scenarios - Miscellaneous

- A software vendor wants you to sign a BAA. You are using their software to teach nursing students unrelated to a healthcare component. Should you sign the BAA?
- Your dental clinic emailed PHI to the wrong email, what do you do now?
- A reporter insists that the patient records in your free clinic are public data because they are not governed by HIPAA. Is this correct?

Practical Scenarios – Miscellaneous (Answers)

- Unless a product supports a covered function, you do not need to sign a BAA, despite what a vendor may insist.
- Any suspected or confirmed data breach must be reported to OGC and System Office IT ASAP.
- Patient records are private data under the MGDPA, even if they are not governed by HIPAA.

Minnesota State Contact Information

Dan McCabe
Assistant General Counsel
daniel.mccabe@minnstate.edu
651-201-1833

Office of General Counsel
https://www.minnstate.edu/system/ogc/index.html

Questions and Answers

- Please chat in your questions.