UW-Madison HIPAA Training (External)

2023-2024

Intended Training Population:

- *This training is for individuals external to UW-Madison. It does not require a NetID. If you have a NetID please take the Internal Training found in Canvas.*
- *You are required to take this course because one of the following applies:*
    - *You are a member of the UW-Madison "workforce" (as that term is defined by HIPAA): you may be a volunteer, teacher, visiting student/intern, or have some other type of unpaid relationship with the UW-Madison Health Care Component*
    - *You are an external research collaborator identified as needing to take UW-Madison HIPAA Training and you do not have a NetID*
    - *You provide Business Associate Services to UW-Madison*

Table of Contents

Lesson 1: Introduction to HIPAA at UW-Madison

What is HIPAA?

"HIPAA" refers to the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).

HIPAA applies to individual healthcare providers (like physicians, nurses, and pharmacists) and to institutional providers (such as hospitals and health systems), and to their workforce,

including students. HIPAA applies to all forms of Protected Health Information (PHI), including paper, electronic, visual, and verbal.

HIPAA is enforced by the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) and State Attorneys General.

There are two (2) key parts to HIPAA:

- **The Privacy Rule** – Establishes national standards for the appropriate use and disclosure of Protected Health Information (PHI).

- **The Security Rule** – Establishes national standards for protecting PHI.

Frequently Asked Questions

How does HIPAA apply to UW-Madison?

UW-Madison is an institutional healthcare provider subject to HIPAA. It is a "hybrid covered entity" for HIPAA compliance purposes.

This means only some areas of campus must comply with HIPAA. The portions of campus subject to HIPAA comprise the UW-Madison Health Care Component (UW HCC).

See HIPAA Policy UW 100 for a complete listing of the areas of campus included in the UW HCC.

Who is included in the UW-Madison Health Care Component (UW HCC)?

All individuals in the units of the UW HCC - including faculty, staff, students, part time personnel, volunteers, and unpaid personnel - are members of the HCC "workforce" for the purposes of HIPAA compliance.

Additionally, members of UW-Madison who don't work for or attend school in the HCC may temporarily be brought into the HCC.

- This occurs when they perform functions for the HCC, including:
    - A project (e.g. a research study or quality assurance project), or

    - An assignment (e.g. a class that requires observing patient care activities)

- These individuals' temporary HCC membership lasts for the duration of such project or assignment.

- And these individuals are required to abide by UW-Madison's HIPAA policies and complete UW-Madison's HIPAA training during this time period.

What is the UW Affiliated Covered Entity?

The UW Affiliated Covered Entity (ACE) is comprised of the following entities or units:

- The units of the UW HCC, except University Health Services, the State Laboratory of Hygiene, and the Athletics Department.

- The University of Wisconsin Hospitals and Clinics Authority.

- The University of Wisconsin Medical Foundation, Inc.

- SwedishAmerican Hospital, including SwedishAmerican Medical Group, SwedishAmerican Home Health Care, and SwedishAmerican Medical Center Belvidere.

- Chartwell-Midwest Wisconsin, LLC and Chartwell-Midwest Wisconsin Health Resources, LLC.

The ACE allows all the entities or units included in it to function as a single entity for HIPAA purposes.

What are the penalties of non-compliance?

Under HIPAA, there are significant fines and penalties for non-compliance.

- Accidental or unintentional violations of HIPAA often involve costly corrective action plans and fines imposed by the federal government.

- Egregious violations of HIPAA laws may lead to criminal proceedings and jail time.

At UW-Madison, unauthorized access to PHI may result in discipline up to and including termination of your employment (for employees) and removal from a clinical experience or expulsion (for students or volunteers).

Failing to comply with HIPAA erodes public confidence and decreases the likelihood patients and research participants will share information openly and honestly with their health care providers. Non-compliance also decreases the likelihood that individuals will authorize use of their information for research purposes.

Check Your Understanding: UW HCC

The Department of Kinesiology, which is not listed as part of the UW HCC (Policy UW-100), is conducting a clinical trial assessing the effect of exercise on study participants with arthritis. The study team includes the following members:

- A professor employed by the Department of Kinesiology.
- A grad student obtaining her Ph.D. in Kinesiology.
- A professor employed by the School of Medicine and Public Health's Department of Medicine.

Question: Is this study subject to HIPAA?

Answer: Yes. The study is subject to HIPAA. Section IX of the UW HCC policy states that studies involving one or more individuals employed within the HCC are subject to HIPAA. Here, the involvement of a professor employed by SMPH's Department of Medicine places the entire study within the UW HCC for the duration of the study and requires the Kinesiology professor and grad student to follow the HIPAA regulations when conducting the study.

Summary

- We are all responsible for complying with HIPAA.
- Complying with HIPAA allows us to be good stewards of patients' and research participants' information.
- Compliance is required by law, helps us avoid penalties, and most importantly: is the right thing to do!

The most important HIPAA compliance principle to keep in mind is to only look at information that you need to do your job and only share information with others that they need to do their job.

Lesson 2: What patient information is protected?

What is protected health information (PHI)?

PHI is any individually identifiable health information created, transmitted, maintained, or received by a HIPAA covered entity relating to the past, present, or future...

- physical or mental health conditions of the individual
- provision of health care to the individual
- payment for health care to an individual

PHI can be in any format - including written, electronic, visual, or verbal.

PHI either contains certain specific identifiers or includes any information with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

HIPAA Identifiers

- Names or initials
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geographical codes.
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical Record numbers
- Health Plan Beneficiary numbers
- Account numbers
- Certificate/License numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers (such as finger and voice prints)
- Full-face photographic images (even if they are partially obscured by eye bars or other means) and any comparable images
- Any other unique identifying number, characteristic, or code that allows identification of an individual, unless otherwise permitted by the Privacy Rule

Please note that shifted dates (i.e. adding a certain number of days to each date in a dataset) are generally still identifiers.

Ask yourself: Where are you likely to encounter PHI in your work?

Items likely to contain PHI

- Medical records - whether paper or electronic
- Research data files/data sets within the UW HCC
- Student course activities related to clinical experiences
- Laboratory reports, such as blood test results
- Pathology sample labels
- Medical bills
- Clinic or research appointment schedules
- Emails to or from current or potential patients or research participants
- Radiologic images (e.g. MRI, CT, X-ray)
- Videos or photos taken during clinical interactions
- Videos or photos taken which show a unique tattoo or other identifying mark

Check Your Understanding

Consider the following situations and determine if they are likely to contain PHI or not likely to contain PHI.

1. An email to a physician from a pharmaceutical rep
2. A CT scan
3. A clinical study's public website
4. A photo of a patient's rash where a tattoo is visible

Answers: PHI – 2, 4; not PHI – 1, 3.

HIPAA's 18th Identifier

- This refers to any unique identifying number, characteristic, or code which could be used in combination with other information to identify an individual. Unique identifying information may include:

- Membership in a sports team during a certain year.

- An individual's involvement in an incident that received publicity- such as a car accident, assault, or workplace injury.

- Membership in a small religious or ethnic population within a certain geography.

- Employment in a certain role - such as a marching band director, the owner of a certain business, a university chancellor, or an elected official.

What is not considered PHI?

A common misconception is that all health information is PHI. What is not considered PHI under HIPAA?

- Information that was PHI, but has been stripped of all the HIPAA identifiers (i.e. de- identified health information).

- Health data that is not shared with a covered entity.
    - Example: A person's heart rate readings on their personal health tracker.

- Health information in the employment records of a covered entity.

Limited Data Sets (LDS) of PHI

A Limited Data Set (LDS) of PHI is data which includes only the identifiers listed below. Limited Data Sets of PHI may be used or disclosed for purposes of research, public health, or healthcare operations without obtaining either an individual's authorization or a waiver or an alteration of authorization for its use and disclosure - so long as a Data Use Agreement is entered into between the provider and the recipient of the LDS of PHI.

Limited Data Sets of PHI can only include:

- City, state, or 5-digit zip code
- Dates
- Other numbers, characteristics, or codes which are not direct identifiers

Limited Data Sets of PHI are still PHI and must be maintained securely and used with systems, tools, and applications approved for use with PHI.

Check Your Understanding

Consider the following six (6) situations and determine if they are PHI or not PHI.

1. A patient's blood test results contained in an after-visit summary.
2. A medical history form completed by a clinical trial participant.
3. A list without identifiers of lab values for all patients within a given year.
4. A county's report of vaccination rates.
5. A bill or statements for a patient's mental health visit.
6. A social media post by a patient about their recent surgery.

Answers: PHI – 1, 2, 5; not PHI – 3, 4, 6.

Summary

Now that you know what PHI is and is not, in the next lesson, you'll learn about its proper use and disclosure.

Lesson 3: Using and Disclosing PHI

When can I share PHI?

Under HIPAA, a covered entity **may not *use*** or ***disclose*** protected health information, except as permitted or required.

- **Use:** Sharing, employment, application, utilization, examination, or analysis of individually identifiable health information ***within*** an entity that maintains such information.

- **Disclose:** Release, transfer, provision of, access to, or divulging in any other manner of information ***outside*** the entity holding the information.

HIPAA allows Covered Entities such as UW-Madison to use and disclose PHI *without authorization* for the following purposes:

- Treatment
- Payment
- Health Care Operations (e.g. certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment)
    - To qualify as genuine health care operations activities under HIPAA quality assurance/improvement, activities need to be structured, documented, and connected to your department's quality assurance/improvement infrastructure.

Researchers may also use PHI without authorization for limited "preparatory to research" activities including:

- Development of research questions (preparation of a grant or protocol).
- Development of eligibility (inclusion and exclusion) criteria.
- Determination of study feasibility.
- Determination of eligibility for study participation of individual potential participant.

Prior to using PHI for these activities, you must complete the "Preparatory to Research Certification" located at UW-Madison's "HIPAA – Researchers" webpage

Special Circumstances

Public Disclosures

For disclosures of PHI in social media posts, journal articles, presentations, news stories, or documentaries, written authorization from the patient or research participant involved must be obtained in advance even if access is limited to members of an academic or professional organization.

Authorization forms are available at UW-Madison's HIPAA website.

News Media Requests

For disclosures of PHI involving news or media production companies are involved, you must first contact your local HIPAA Privacy Coordinator, the HIPAA Privacy Officer, or UW Health's Media Relations team (if UW Health facilities are involved).

Those individuals will ensure appropriate involvement of all stakeholders to address privacy, security, infection control, intellectual property, and other liability concerns.

Government Requests

HIPAA permits (but does not mandate) certain other disclosures of PHI without authorization for public health activities, workers' compensation, and specialized government functions. Those situations are too specific to explain in this training.

If you have questions about a specific situation, contact the UW Madison HIPAA Privacy Officer.

How much PHI should I share?

The “Minimum” Necessary Standard

When you use or disclose PHI, you must use or disclose only the minimum amount of PHI necessary to accomplish your intended purpose.

This “minimum necessary” standard is designed to limit unnecessary or in appropriate access to and disclosure of PHI while also accommodating legitimate business or educational needs to use certain information.

The “minimum necessary” standard does not apply when:

- PHI is used or disclosed for **treatment** purposes.
- PHI is disclosed **to the patient** or the patient's legally authorized representative.
- PHI is disclosed **pursuant to a valid HIPAA authorization**.
- The disclosure is **required by law**.

Refer to HIPAA Policy UW-109 for more information about this standard.

Check Your Understanding

Consider this scenario:

You have just completed data collection for a research study and are beginning to analyze the data. You don’t anticipate needing any identifiers for data analysis.

Answer the following three (3) questions:

1. What step should you take to ensure compliance with HIPAA's "Minimum Necessary" requirement?
    a. Code the data and store the identifiers separately for later use if needed.
    b. Leave only participants' first names in the spreadsheet.
    c. Leave only participants' mailing address in the spreadsheet.
    d. Leave participants' names and contact information in the spreadsheet with the data, because it may be needed later.

2. After removing participant contact information from the dataset, the following fields remain: dates of study visits; participants’ diagnosis; and lab values from study visits. Under the HIPAA regulations, what is this data set classified as?
    a. De-identified health information (i.e. not PHI)
    b. Limited Data Sets (LDS) of PHI
    c. PHI exceeding a LDS

3. Finally, you need to share this LDS with a collaborator at another university who is also going to assist with data analysis. Select ALL the steps that need to be completed before sending them the data.
    a. Ensure that an agreement is in place between both institutions that is signed by individuals with signatory authority and includes the HIPAA Data Use Agreement (DUA) terms.
    b. Confirm that the IRB protocol allows sharing data with this individual.
    c. Identify an approved tool for securely sending this information to the collaborator.
    d. Ensure the collaborating institution is paying for the time spent creating the LDS.

Answers: Question 1 – a; Question 2 – b; Question 3 – a, b, c.

How should you use or disclose PHI?

In addition to accessing PHI appropriately and complying with the "minimum necessary" standard, there are other considerations you must keep in mind when using or disclosing PHI.

Social Media and PHI

Exercise caution when considering sharing patient or research participant information on social media.

- Personal identifiers or unique circumstances should not be shared unless you have obtained patient or participant authorization prior to posting.

- Work with your Marketing and Public Relations colleagues who maintain official social media accounts to publicize success stories or patient care experiences. These teams must assist with compliance, branding, and strategy prior to posting.

- Before sharing any information about a research participant's care or experience, consult your HIPAA Privacy Coordinator, the HIPAA Privacy Officer, or your reviewing IRB to ensure publicity is acceptable under your approved research protocol - you may need to request a "change of protocol" in addition to obtaining the research participant's authorization in advance of any publicity.

Handling and distributing paper documents with PHI

- When you handle paper documents containing PHI (such as clinical after-visit-summaries, discharge instructions, or a signed consent form copy), double-check to make sure you distribute the information to the correct person.

- Be conscious of the PHI you may need to carry with you to avoid inadvertently leaving it in a public area.

- Shred PHI when you no longer need it.

- If you fax PHI for any reason, call or email the recipient to confirm the number is correct.

Mailing PHI

When you mail information to patients, research participants, or individuals participating in quality improvement projects:

- DO NOT USE POSTCARDS unless approved by UW-Madison's Privacy Officer.
- NEVER use return address blocks or envelopes which reference sensitive or potentially-stigmatizing diagnoses, conditions, or therapies such as Alzheimer's disease, substance abuse disorder, HIV/AIDS, or mental health conditions.
- Ask UW-Madison's Privacy Officer to review materials you intend to mail for research or quality improvement purposes if they are not reviewed by an IRB.
- Use "window envelopes" to avoid mislabeling envelopes which contain personalized letters.
- Work with a mass-mail service if mailing a high volume of materials.
    - Contact the HIPAA Privacy Officer for information about mail service vendors that have established Business Associate Agreements with UW-Madison.

How do you safeguard PHI?

You are required to safeguard the privacy and security of PHI.

Key ways to do this include:

- Limit your risk by working with de-identified information or Limited Data Sets of PHI.
- Access PHI in accordance with the "minimum necessary" standard.
- Exercise care when using and disclosing PHI.
- Comply with UW-Madison's HIPAA Policy UW 129 about E-mail Communications Involving Protected Health Information.
- Use tools and applications approved for use with PHI.

Special Considerations for Research

If you conduct research using PHI, familiarize yourself with UW-Madison's HIPAA policies and procedures applicable to your research.

- Research resources are available on the HIPAA - Resources webpage through the Office of Compliance.
- Human Subjects Research regulations (the "Common Rule") and HIPAA have different requirements, especially about coding of data - contact your HIPAA Privacy Coordinator with questions about these requirements.

Research and projects that don't require IRB review still must comply with HIPAA!

Research Reviewed by an External IRB

If conducting research using PHI that's reviewed by an external IRB, you must verify if that external IRB provides "Privacy Board" review to evaluate compliance with HIPAA.

- If the external IRB does not provide Privacy Board review, contact the Reliance and Navigation Team at irbreliance@wisc.edu or the HIPAA Privacy Officer to initiate review of your research for HIPAA compliance.

- The UW-Madison Health Sciences IRB provides Privacy Board review in accordance with UW-Madison HIPAA Policy UW-113, Designation of IRBs as Privacy Boards.

De-Identified Health Information

Data which has been de-identified no longer qualifies as PHI and is not subject to HIPAA. When you work with de-identified data you no longer need to obtain an individual's authorization to use or disclose the PHI, and you can more freely share the information. Refer to HIPAA Policy UW-114 for additional details.

- "Safe Harbor" de-identification can be accomplished by removing the 18 HIPAA identifiers from the information you work with. Removing all identifiers can be challenging - especially if your data includes unique elements such as athlete status and sport played, a genetic condition, or a specific type of occupation or injury. HIPAA Policy UW-114 also requires validation of de-identification by campus HIPAA staff for certain types of data when that data is being sent outside the HCC or ACE.

- "Expert Determination" de-identification requires consultation and documentation by an expert in statistical and scientific principles and methods for rendering information not individually identifiable.
    - **Note: UW-Madison does not currently have staff in-house to provide de-identification by expert determination.**

Contact the SMPH Honest Broker or the HIPAA Privacy Officer for more information.

Check Your Understanding

Read the following two (2) scenarios and respond to the questions.

Scenario 1:

You are conducting a study in which the participants have been recruited from UW-Madison sports teams. The data for each participant is limited to the following elements:

- Sport played
- Gender
- Height
- Weight

- Number of previous upper body injuries
- Number of previous surgeries

Question: Under the HIPAA regulations, is this data de-identified?

Answer: No. This is not de-identified data because a person could use the data provided and publicly available information, such as the team roster, to quickly identify a participant.

Scenario 2:

You are working on a study in which electroencephalography (EEG) data has been collected from clinical trial participants. The study principal investigator (PI) has told you that they have personally confirmed the data is de-identified.

Question: Under campus policy, should you consider this data properly de-identified?

Answer: No. The PI's statement is not enough. You need to obtain validation of de-identification from one of the individuals specified in UW-114 De-Identification of Protected Health Information Under the HIPAA Privacy Rule.

Lesson 4: Working with Electronic PHI (ePHI)

Unauthorized access to PHI may result in discipline up to and including termination of your employment (for employees) or removal from a clinical experience or expulsion (for students or volunteers).

Accessing PHI in Electronic Systems

UW-Madison grants role-based access to electronic systems containing PHI in accordance with the requirements of the HIPAA Security Rule. Access to PHI is permitted only if your role or job requires you to access it to perform the functions of your role. Your electronic access to PHI comes with a unique username and password.

- NEVER access PHI using another individual's username and password.

- ONLY access PHI to perform the functions of your role.

It is a violation of UW System and UW-Madison policies to access PHI using another individual's credentials or to share your credentials for another individual's use to access PHI.

Unless you have a legitimate business or educational need to do so - NEVER access medical records of:

- A relative including a child, a current or previous spouse, or other family member.
    - Treatment is not generally an appropriate reason to access a family member's medical record. UW Health Policy 1.2.23 broadly prohibits the use of UW Health resources (including Health Link) to treat family members.

- A friend, neighbor, coworker, or acquaintance.

- A celebrity, high profile figure, or someone you learn about in news media such as political figures, community leaders, or individuals involved in accidents reported in the news.

Your own curiosity, desire to learn about a particular health condition, or interest in how a former patient or research participant is doing are NOT legitimate reasons to access PHI.

Contact your supervisor, course instructor, or the HIPAA Privacy Officer if you have questions about accessing information for educational, quality improvement, or other purposes.

Accessing PHI in Health Link

If you have access to UW Health's electronic medical record (known as "Health Link"):

UW Health allows you to view (but not print or change) your own medical records - but not the records of ANY other individual in the absence of a work-related or educational need to do so.

Note: ** This is a UW-Madison and UW Health policy. Other health systems, including UPH Meriter, do not allow any access which is not work-related.

You MAY NOT use your access to review others' PHI anywhere in Health Link without a legitimate work related or educational need to do so - even for individuals for whom you are a parent, legal guardian, or legal healthcare decision maker. This applies regardless of where in Health Link you access PHI (i.e., even viewing an Identity Report is not permitted without a legitimate work related or educational need to do so).

Non-work or non-educational access to others' UW Health medical records must occur via MyChart or through the Health Information Management department of UW Health.

Audits of Access to PHI in Health Link

UW-Madison and UW Health actively monitor the use of Health Link and collaboratively investigate audit findings to ensure access to PHI is appropriate. Audits of access to PHI:

- Are performed on a routine basis.
- May be prompted by complaints from patients, research participants, or employees.
- Can go back many years and include details on every Health Link record a user accessed.

You may be contacted by privacy staff seeking more information about audit findings.

Inappropriate access to Health Link may result in disciplinary action by UW-Madison and UW Health.

Prevent Misuse of Your Credentials

You are responsible for access into any patient or research participant records made under your username and password. Be sure you:

- Use strong passwords.
- Avoid writing out your usernames and passwords.
- Log out of your computer or lock your workstation whenever you leave it unattended.
- Do not share your passwords.

Tools Approved for Use with PHI

A list of approved tools for use with PHI is available on the UW-Madison Office of Compliance website and is updated periodically to add or remove tools as appropriate.

Consult this list prior to using a tool with PHI. Failure to do so can result in a HIPAA incident.

Tools NOT Approved for Use with PHI

If you become aware of PHI being used with any tools not listed as approved, including the following examples, please report the activity using the online HIPAA Incident Report Form (discussed later in this training):

- Google Workspace Tools (e.g. Gmail, GoogleCalendar, GoogleDocs, GoogleSheets)
- Personally acquired software or tools (e.g. email accounts, file-sharing accounts, and instant messaging accounts)
- Social Media (e.g. Facebook, Twitter, Instagram, Snapchat) or their Messaging Tools
- Canvas

Forwarding email that contains PHI to an address in an unapproved third party domain (such as gmail.com, me.com, or charter.net) violates HIPAA as well as UW-Madison and UW Health policies.

Using unapproved email domains can result in breaches which require notification to the impacted individual(s), the federal government, and the media; because each instance of emailing an individual's PHI is considered an unauthorized disclosure to third party email service provider.

Emailing PHI

HIPAA and UW-Madison policy address the appropriate use of email with PHI:

- Patients should be encouraged to use patient portals provided by their health care providers for clinical communications (such as MyChart or the MyUHS portal).
- Email may be sent without applying other security controls to other “wisc.edu” addresses or to external email addresses within approved domains.
- Email with research participants must follow current IRB Guidance on the Use of Email for Research.
- Email may only be auto forwarded by rule to approved domains.

See HIPAA Policy UW-129 for additional information about emailing PHI.

Best Practices for Emailing PHI

Reduce privacy and security risks to the PHI you email with these best practices:

- Consider whether better methods exist for sharing the PHI involved.
- Use shared network drives, Secure Box Folders, or other collaboration tools approved for use with PHI when routinely sharing PHI with others for work or research purposes.
- Empty your “Deleted Items” folder periodically to fully delete PHI you receive or send and no longer need or configure your email account to automatically empty the folder (see the Office 365 KnowledgeBase page for instructions).
- Review your email lists and frequent contacts to ensure you direct email messages to the correct individuals.
- Use "Bcc" if sending a single email to multiple research participants.
- Do not send spreadsheets or other files containing large amounts of PHI via email.

Cybersecurity Threats in Healthcare

Cybersecurity threats to healthcare entities put patients’ and research participants’ privacy as well as our IT systems at risk. These threats include:

- Email phishing attacks.
- Ransomware attacks.
- Loss or theft of equipment or data.

- Insider, accidental, or intentional data loss.

- Attacks against connected medical devices that may affect patient safety.

Complying with the policies and best practices discussed in this training will reduce the likelihood of these threats impacting the PHI you work with.

Storage and Computing Environments for PHI

To further reduce the likelihood of cybersecurity threats impacting the PHI you work with:

- Access PHI with computers, mobile devices, and other tools maintained and/or managed by IT staff who support your HCC unit.
    - If you are temporarily brought into the HCC for a research project, access PHI with computers, mobile devices, and other tools:
        - Maintained or managed by the unit of the HCC that you are collaborating with on the research, OR
        - Reviewed by UW-Madison Cybersecurity for use with PHI.

- Use computing and data storage tools from UW-Madison's Approved Tools List.

Electronic Calendars

Clinical or Research appointment details must be stored securely only in appropriate and approved tools such as electronic medical records systems or other institutionally endorsed data storage systems.

PHI should NOT be copied from electronic medical or research records into Office 365 calendars or other personal calendars (such as Google Calendars or Apple Calendar).

UW Health allows secure access to clinical schedules from mobile devices via Epic-supplied mobile apps called Haiku and Canto. Mobile devices must be enrolled in UW Health's Mobile Device Management service for access to these resources.

Copying-and-pasting PHI from electronic medical records or research files into electronic calendars jeopardizes the privacy, security, and confidentiality of the PHI.

This is especially true when calendars are shared with other individuals (who may not be authorized to access the PHI), when calendars sync to unmanaged mobile devices, or when UW-Madison does not have a Business Associate Agreement with the vendor of the calendar used.

In these cases, including PHI in your electronic calendars can result in unauthorized disclosures of PHI and HIPAA breaches.

Lesson 5: When HIPAA Requires a Contract to Share Data

Business Associates

Individuals and businesses that provide services which involve the use, storage, analysis, or transmission of PHI on behalf of a Covered Entity are "Business Associates."

- HIPAA requires entering into "Business Associate Agreements" (BAAs) in which the Business Associate agrees to use appropriate safeguards to protect PHI.

- UW-Madison's BAA templates are available in the expandable Forms menu at the HIPAA Policies and Forms webpage.

- In addition to completing a BAA, the Business Associate must be reviewed by the Office of Cybersecurity prior to use for compliance with HIPAA's security requirements.
    - Request a review using the form on the OneTrust webpage.

Using UW-Madison's BAA templates will reduce BAA review and execution timelines!

Third party services that may require a BAA include:

- Cloud-based tools
- Transcription
- Shredding/disposal
- Direct mailing
- Claims administration

BAAs are routed through one of the following Offices:

Office	When…
Purchasing within the Division of Business Services.	a purchase is being made.
Research and Sponsored Programs	related to research projects, route BAAs via WISPER/RAMP with other project documents.
Office of Compliance HIPAA Privacy Officer	there is no purchase being made and the BAA is not related to a research project.

BAAs must be executed by individuals with Board of Regents signature authority (see the Signature Authority Memo at Office of Legal Affairs - Contract Approval).

Business Associate Policies

- See HIPAA Policy UW-116 for details about engaging Business Associates for UW- Madison.
- See HIPAA Policy UW-117 for information about providing Business Associate services for another Covered Entity.

Data Use Agreements

HIPAA allows using or disclosing a Limited Data Set (LDS) of PHI without authorization if the recipient agrees to use the LDS of PHI for specified purposes in the form of a Data Use Agreement (DUA).

DUAs are routed through one of the following Offices:

Office	When…
Purchasing within the Division of Business Services.	a purchase is being made.
Research and Sponsored Programs	related to research projects.
Office of Compliance HIPAA Privacy Officer	there is no purchase being made and the DUA is not related to a research project.

Using approved Data Use Agreement (DUA) templates will reduce DUA review and execution timelines!

Federal Demonstration Partnership (FDP) templates are preferred for research projects.

Reminder

DUAs must be executed by individuals with Board of Regents signature authority (see the Signature Authority Memo at Office of Legal Affairs - Contract Approval).

- See HIPAA Policy UW-115 for details about LDSs of PHI and DUAs.

Data Transfer and Use Agreements

Even where HIPAA may not require a contract to share data externally, UW-Madison may require a Data Transfer and Use Agreement (DTUA) to protect the rights of the subjects of the data and the University's interest in the value of the data.

Please consult the Research and Sponsored Programs website for more details and DTUA templates.

Lesson 6: HIPAA Incidents and Breaches

Any time you suspect that the loss, theft, or misdirection of PHI has occurred, immediately complete a HIPAA Incident Report Form.

HIPAA Incident Reporting

Completing a UW-Madison HIPAA Incident Report Form is crucial so the incident can be investigated and addressed promptly.

- Time is of the essence!
- Each member of the UW HCC workforce has a duty to report a known or suspected HIPAA Incident immediately upon learning of the incident.
- Federal regulations require UW-Madison to investigate all HIPAA Incidents and, in some cases, provide timely Breach Notifications to affected individuals, the Oice for Civil Rights (OCR), and if 500 or more individuals affected, the media.

Examples of HIPAA Incidents to Report

- IT vulnerabilities caused by phishing, hacking, failure to update operating systems or applications, incorrect configuration of website settings, etc.
- Loss or theft of a workforce member's laptop or mobile device used with PHI.
- Use of unapproved web-based tools or applications.
- Receipt or sending of misdirected mail, email or faxes including PHI.
- Receipt or sending of PHI which is more identifiable than intended without patient/research participant authorization.
- Suspected password-sharing or compromised usernames/passwords.
- Discovery of an unattended and unsecured workstation.
- Inappropriate sharing or publication of images which contain PHI - either within the image or as metadata incorporated in the image file.

Questions about Incident Reporting?

If you have questions about a possible HIPAA Incident you'd like answered before completing the online HIPAA Incident Report Form, do one or more of the following:

- Speak with your supervisor or instructor.
- Call or email your unit's HIPAA Privacy or HIPAA Security Coordinator.
- Call or email the UW-Madison HIPAA Privacy or HIPAA Security Officer.
- For research related incidents, contact the anonymous Human Research Protection Program Hotline at 608-890-1273.
- Call your department's IT personnel or the DoIT Help Desk at 608- 264-HELP (4357) if the incident involves a technical matter - such as theft of a mobile device, loss of an external hard drive, malware, or a phishing attempt.

Check Your Understanding

Consider the following situations and answer the associated questions.

1. You are a researcher on a sponsored, multi-site study and you overheard a study team member stating they shared a data set of PHI with a collaborator at another site. You're not sure that all the needed steps were taken to share this data prior to it being sent to the collaborator. **Which of the following are appropriate actions you can take? Select all that apply.**
    a. Speak with your supervisor or instructor.
    b. Submit a HIPAA Incident Report via the Office of Compliance website.
    c. Contact your unit's HIPAA Privacy and/or Security Coordinator(s).
    d. Contact the UW-Madison HIPAA Privacy and/or Security Officers.
    e. Document the incident by placing a note in the affected participant's research file and take no further action.

2. A study team at UW-Madison sent out a letter to approximately 700 research participants enrolled in a study on dementia informing them of an upcoming study visit. The study team did not use window envelopes, resulting in the letters and envelopes getting mismatched. As a result of this error, participants received letters intended for other participants, effectively informing them of the identities and dementia diagnoses of fellow participants. The study team reported this incident to the HIPAA Privacy Officer who determined the incident met the definition of a HIPAA Breach. **What are the University's obligations under HIPAA's Breach Notification Rule? Select all that apply.**
    a. Report breach to HHS's Office for Civil Rights (OCR).
    b. Notify media because over 500 individuals were affected.
    c. No obligation to notify participants or media because fewer than 1,000 individuals were affected.
    d. Notify individual participants of the breach of their PHI.

3. **What effects will this breach likely have on the study team?** Select all that apply.
    a. Time, effort, and money expended on addressing the breach.
    b. Existing participants dropping out of the study.
    c. Lost opportunity (e.g. inability to recruit additional study participants due to time spent on breach mitigation).
    d. Reputational loss (e.g. fewer eligible participants agreeing to enroll).

Answers*:* Question 1 – a, b, c, d; Question 2 – a, b, d; Question 3 – a, b, c, d.

Lesson 7: New Resources

There are some new resources related to working with HIPAA:

- NIH Data Management Guidance
    - **Note**: This requirement doesn't supersede HIPAA and allow for the sharing of data that wouldn't otherwise be shareable under the HIPAA regulations.

- UW-Madison Risk Management and Compliance (RMC) website

- Accounting for Disclosures Guidance

Lesson 8: HIPAA Resources and Support

- OCR's HIPAA resources are available on the Health Information Privacy page through the U.S. Department of Health and Human Services.

- For information about HIPAA at UW-Madison, visit the HIPAA (Health Insurance Portability and Accountability Act) page through the Office of Compliance.

- To request Health Link data for research, fill out the form on UW-Madison's ICTR CHI2 Consultation page.

- For questions about this training or the online resources that are referenced, please contact your unit's HIPAA Privacy or Security Coordinator.
    - **Privacy Coordinator**s can assist with issues such as data classification, appropriate use of PHI, external sharing of PHI, HIPAA-related contracts, and HIPAA Privacy policies and procedures.
    - **Security Coordinators** can assist with issues such as departmental and new tool risk assessments, appropriate tools and systems for working with PHI, and HIPAA Security policies and procedures.

- UW-Madison's HIPAA Privacy Officer and HIPAA Security Officer are also available to assist with HIPAA inquiries and are often involved in navigating more complex HIPAA issues.

Completing this Course

You are almost done. Click https://uwmadison.co1.qualtrics.com/jfe/form/SV_9RWd6eES96i5wqi to complete your final step in the training process. Thank You!

Please note: Printable certificates are not generated for this training.