UW-Madison HIPAA Training

2022-23 ACADEMIC YEAR

HIPAA Training for Individuals External to UW-Madison
Does NOT Require a UW-Madison NetID
Trainee Population

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, preceptor, teacher, 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

This training course is estimated to require 20-25 minutes to complete and does not contain audio or animations. With technical questions, please contact help@doit.wisc.edu or call 608-264-HELP (608-264-4357).
Why do I have to do this every year?

HIPAA and UW-Madison’s HIPAA Training Policy require training all members of the UW-Madison “workforce” before they gain access to protected health information, and on an annual basis thereafter. Workforce members who do not work with protected health information are trained annually.

This training reinforces topics covered in previous training and provides information about new resources developed since the creation of our prior training course.

As always: Contact UW-Madison’s HIPAA Privacy or Security Officers or your local HIPAA Privacy or Security Coordinator with questions.

Contact information is available at compliance.wisc.edu/hipaa/coordinators/.

Thank you!
“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).

It applies to individual healthcare providers (like physicians, nurses, 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” – described in more detail later), including paper, electronic, visual, and verbal.

HIPAA is enforced by the Office for Civil Rights (OCR) and State Attorneys General.

OCR’s HIPAA resources are available at: hhs.gov/ocr/privacy/

For information about HIPAA at UW-Madison, visit compliance.wisc.edu/hipaa.
UW-Madison is a hybrid institutional healthcare provider subject to HIPAA; 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). UW-Madison policy [UW-100 (HIPAA Policy 1.1)] lists the areas of campus included in the UW HCC.

All individuals who work, volunteer, or attend school in/for units of the UW HCC are required to comply with HIPAA.

Individuals external to UW-Madison become part of the UW HCC when they perform functions such as:
- Serving as a preceptor for a unit of the UW HCC (including zero-dollar appointees)
- Working on research studies
- Collaborating on quality improvement projects
- Volunteering on research, outreach, or education/training projects
What are the penalties for non-compliance?

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

Even accidental or unintentional violations of HIPAA may involve 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 employment (for employees) and removal from a clinical experience or expulsion (for students).

Not complying with HIPAA erodes public confidence and decreases the likelihood patients and research subjects will share information openly and honestly with their health care providers.

In the preceptor context, non-compliance may also have a negative impact on a student’s/trainee’s experience and may also create privacy or security challenges for a health care organization where a student/trainee completes a clinical rotation.
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!
What is PHI?

PHI stands for “Protected Health Information.” It is any individually-identifiable health information created, transmitted, maintained, or received by a health care provider relating to any of the following:

- The past, present, or future physical or mental health conditions of the individual
- The past, present, or future provision of health care to the individual
- The past, present, or future payment for health care to an individual

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

PHI can be in any format – including written, electronic, visual, or verbal.
### HIPAA Identifiers

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Names or Initials</td>
</tr>
<tr>
<td>2.</td>
<td>All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geographical codes</td>
</tr>
<tr>
<td>3.</td>
<td>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</td>
</tr>
<tr>
<td>4.</td>
<td>Telephone Numbers</td>
</tr>
<tr>
<td>5.</td>
<td>Fax Numbers</td>
</tr>
<tr>
<td>6.</td>
<td>Email Addresses</td>
</tr>
<tr>
<td>7.</td>
<td>Social Security Numbers</td>
</tr>
<tr>
<td>8.</td>
<td>Medical Record numbers</td>
</tr>
<tr>
<td>9.</td>
<td>Health Plan Beneficiary Numbers</td>
</tr>
<tr>
<td>10.</td>
<td>Account Numbers</td>
</tr>
<tr>
<td>11.</td>
<td>Certificate/License Numbers</td>
</tr>
<tr>
<td>12.</td>
<td>Vehicle Identifiers and Serial Numbers, including License Plate Numbers</td>
</tr>
<tr>
<td>13.</td>
<td>Device Identifiers and Serial Numbers</td>
</tr>
<tr>
<td>14.</td>
<td>Web Universal Resource Locators (URLs)</td>
</tr>
<tr>
<td>15.</td>
<td>Internet Protocol (IP) Address Numbers</td>
</tr>
<tr>
<td>16.</td>
<td>Biometric Identifiers, Including Finger and Voice Prints</td>
</tr>
<tr>
<td>17.</td>
<td>Full Face Photographic Images and Any Comparable Images</td>
</tr>
<tr>
<td>18.</td>
<td>Any other unique identifying number, characteristic, or code that allows identification of an individual, unless otherwise permitted by the Privacy Rule</td>
</tr>
</tbody>
</table>
Examples of PHI

- Medical records – whether paper or electronic
- Research data files/data sets which include HIPAA identifiers
- Student course activities which include HIPAA identifiers
- Laboratory reports, such as blood test results
- Pathology sample labels
- Hospital bills
- Clinic or research appointment schedules
- Emails to or from patients or potential research participants that include details about their health-related conditions
- MRI scan data
- Videos or photos taken during clinical or instructional interactions
- Videos or photos showing a unique tattoo or other identifying mark
HIPAA’s “18th identifier” 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 – due to media attention when members of the team experienced injuries
- How an individual was injured – such as during a car accident, assault, or workplace injury which received publicity
- Patient care location and time of admission – such as the place the patient arrived for treatment along with the date and time of day
- 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 public official
Using and Disclosing 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
Using and Disclosing PHI (cont’d)

HIPAA allows entities subject to HIPAA to use and disclose PHI without authorization for:

- Treatment
- Payment
- Health Care Operations (administrative, financial, legal, QI, training activities)

When you use or disclose PHI for payment or health care operations purposes, you must use and disclose only the minimum amount of PHI necessary to accomplish your intended purpose.

This “Minimum Necessary” Standard is designed to limit unnecessary or inappropriate access to and disclosure of PHI – while also accommodating legitimate business or educational needs to use certain information.
Minimum Necessary Standard

The “Minimum Necessary” Standard does not apply in the following circumstances:

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

Refer to [UW-109 (HIPAA Policy 3.8)](UW-109(HIPAA_Policy_3.8)) for more information about this standard.
In addition to accessing PHI appropriately and with the Minimum Necessary Standard in mind, you must be careful when you use or disclose PHI.

- When you handle hard-copy PHI (such as clinical after-visit-summaries, discharge instructions, or research study questionnaires), double-check to make sure you hand or mail the information to the correct person.

- Be conscious of the hard-copy PHI you carry with you (if any) to avoid inadvertently leaving or losing it in a public area. Shred hard copies of PHI when you no longer need them.

- If you fax PHI for any reason, verify the fax number to make sure the number is correct. If you have not recently faxed PHI to the intended recipient, call or email the recipient to confirm the number.
Safeguarding PHI

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

Several ways to do this include:

▪ Limiting your risk by working with de-identified information or Limited Data Sets of PHI (discussed in the following two slides)

▪ Accessing PHI in accordance with the Minimum Necessary Standard

▪ Exercising care when Using and Disclosing/Sharing PHI

▪ Complying with UW-Madison’s [UW-129 (HIPAA Policy 8.6)] about E-mail Communications Involving Protected Health Information (discussed later with HIPAA Policy Updates)

▪ Use tools and applications approved for use with PHI (discussed later with New Resources)
If you Supervise Trainees...

You should ensure trainees appropriately access, use, or disclose PHI they encounter during their clinical rotations.

Several ways to do this include:

▪ Making sure they follow the Minimum Necessary Standard

▪ Monitoring for appropriate use of and access to PHI within electronic systems

UW-Madison Health Sciences Students are trained to understand they may only access PHI to the extent necessary to perform the functions required of them during their clinical training. They should only access PHI of individuals to whom they are assigned, and should only access to PHI using their own usernames and passwords.

As a preceptor, you should model appropriate use of PHI. If you are ever uncertain about UW-Madison’s policies about accessing PHI, the UW-Madison HIPAA Privacy Officer or the HIPAA Privacy Coordinator for the area of campus you interact with can provide assistance.
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](http://example.com) for additional details.

- **“Safe Harbor” de-identification** can be accomplished by removing the 18 HIPAA identifiers (listed earlier) 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.

- **“Expert Determination” de-identification** requires consultation and documentation by an expert in statistical and scientific principles and methods for rendering information not individually-identifiable. *UW-Madison does not currently have experts in-house to provide this level of de-identification.*

Contact the [SMPH Honest Broker](http://example.com) or the [HIPAA Privacy Officer](http://example.com) for more information.
Limited Data Sets of PHI

A Limited Data Set (LDS) of PHI is data which includes limited identifiers. LDSs of PHI may be used or disclosed for purposes of research, public health, or health care 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 (discussed later in the training).

Limited Data Sets of PHI may include:

▪ City, state, or 5-digit ZIP Code

▪ Dates

▪ Other numbers, characteristics, or codes which are not direct identifiers

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

HIPAA and UW-Madison policy allow certain email communications 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 information about emailing PHI

*Requires NetID Authentication
In addition to HIPAA Policy Requirements, you can reduce privacy and security risks to the PHI you email by implementing 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

- If sending a single email to multiple research participants, use “Bcc”
Maintaining patients’ and research participants’ privacy is a fundamental ethical and legal obligation of each member of the UW HCC workforce.

- You must be mindful of privacy and confidentiality in digital and virtual environments
- Be careful about the level of detail you share in personal social media posts
- Work with your Marketing and Public Relations colleagues who maintain official social media accounts to publicize “success stories” or “patient care experiences” – they can assist with compliance, branding, and strategy
- 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
Current Cybersecurity Threats in Healthcare

Cyber threats to healthcare entities put patients’ and research subjects’ privacy as well as IT systems at risk. Current cybersecurity 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 when engaged in your clinical, teaching, educational, or research duties.
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 trained IT staff who support your unit of Health Care Component (HCC)
  - 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
    - That have been reviewed by UW-Madison Cybersecurity for use with PHI

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

- Use Research Cyberinfrastructure services appropriate for PHI when conducting research (contact the Research Cyberinfrastructure team at rci@g-groups.wisc.edu for support)
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 or scheduling systems.

- PHI should **not** be copied from electronic medical records into Office 365 calendars or other personal calendars (such as Google Calendars or iCal).

- 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. See [https://uconnect.wisc.edu/depts/uwhealth/information-services/uw-health-mobile-device-management/](https://uconnect.wisc.edu/depts/uwhealth/information-services/uw-health-mobile-device-management/)
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.
- If a UW-Madison Business Associate leverages technology to provide services, the technology must be reviewed by the Office of Cybersecurity for compliance with HIPAA’s security requirements – request review using the form on the OneTrust webpage (requires NetID authentication).
Companies that qualify as Business Associates under HIPAA may include:

- Cloud-based Service Providers
- eFax Solution Providers
- Transcriptionists (such as those who transcribe research interviews)
- Media Sanitization Vendors
- Shredding / Disposal Companies
- Direct Mail Services (such as those used to send research recruitment mailings)
- Third-party Claims Administrators
BAAs are routed through one of the following Offices:

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

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

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

- **Using approved DUA templates will reduce DUA review and execution timelines!**
  - Federal Demonstration Partnership (FDP) templates are preferred for research projects

- 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
Policy and Resource Updates to Support HIPAA Compliance
HIPAA Policy Updates

**HIPAA Policy UW-114** (De-Identification of Protected Health Information Under the HIPAA Privacy Rule) was updated to achieve readability and make the following substantive changes:

- Clearly articulate that de-identification can be achieved through either the “Safe Harbor Method” or the “Expert Determination Method.”

- Indicate that “other information” beyond the 18 HIPAA identifiers may also need to be removed from a data set to achieve de-identification under the Safe Harbor Method. Examples of such other information are provided at Section II.A., and include factors such as athlete status, a unique occupation such as a judge or politician, or details about a situation which received media attention.

- Add a requirement for validation of de-identification in higher-risk situations – which are enumerated in Section II.C.
New HIPAA Policy

**HIPAA Policy UW-133** (Remote Access to Protected Health Information) was implemented in 2021 to address issues surrounding the increased need for workforce members to access PHI remotely

- Requires departments to more closely monitor or approve endpoints and mobile devices used at remote locations

- For departments to accomplish this requirement, they will need to explore how to implement the campus **Endpoint Management Policy (UW-526)**, including the standards that are in development and mobile device management solutions
New HIPAA Policy

**HIPAA Policy UW-136** (Workstation and Mobile Device Use and Security Configuration) was implemented in 2021 to address issues surrounding the increased need for workforce members to access PHI remotely

- **Departments must ensure their assets meet the best practices that will be outlined in this policy’s procedure**

- **All users are responsible for protecting the privacy, security, confidentiality, integrity, and availability of PHI in the information systems in which they work at all times**

- **Unmanaged Mobile Devices must not be used to access PHI**
Resource Update: Approved Tools

- UW-Madison and UW Health Approved Tools for Exchanging and/or Storing Protected Health Information (Approved Tools List) is updated periodically as needed.

- Most recent update in April 2022 included:
  - Changes made to enhance readability and provide additional clarity
  - Approved Tools Added:
    - Globus
    - Secure Zoom
    - Platform X
Reminder: Tools NOT Approved for Use with PHI

If you become aware of PHI being used with any of the following products, 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
**Resource Update: Data Sharing Guidance**

**Guidance** was recently published to address common questions about sharing Human Subjects research data.
Guidance was also recently published to address common questions about receiving Human Subjects research data from external entities.
The UW-Madison Office of Cybersecurity has updated its online resources to assist users with common issues surrounding HIPAA security

- Visit [Cybersecurity Risk Management and Compliance](#) for background information related to their processes, including risk assessments for new tools and systems

- Visit [UW-Madison’s HIPAA Security program](#) for resources related to:
  - HIPAA Security requirements
  - HIPAA Security polices
  - Security Review request form
  - SecureBox request form
HIPAA Incidents & Breaches
Unfortunately, accidents and mistakes with PHI happen. Any time you suspect that an incident involving the loss, theft, or misdirection of PHI has occurred, immediately complete a HIPAA Incident Report Form so the incident can be investigated and addressed promptly.

- Time is of the essence! (especially when an incident involves suspected IT security vulnerabilities or theft of a mobile device)
- UW-Madison’s HIPAA Incident Report Form is available online at compliance.wisc.edu/hipaa
- 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 and document the investigation of all HIPAA Incidents, and might also require Breach Notifications (to affected individuals, news media, and OCR) within a specific timeline
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 emails or faxes which include PHI
- Receipt or sending of PHI which is more identifiable than intended without patient/research participant authorization
- Suspected password-sharing or compromised usernames/passwords
- Unintended sharing or publication of images which contain PHI – either within the image or as metadata incorporated in the image file
Find Answers to Questions About Incident Reporting:

If you have questions about a possible HIPAA Incident you’d like to address before completing the online HIPAA Incident Report Form, take one or more of the following actions:

▪ 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 (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
This training will remain accessible to you through Canvas, and your completion will remain valid, until the release of the next HIPAA training course during the 2023-24 academic year.

- For questions this training or the online resources referenced in it could not answer, please contact your unit’s HIPAA Privacy or Security Coordinator first
  - Privacy Coordinators 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
You are almost done....

Click here* to complete your final step in the training process.

Thank You!!

* Copy and paste this URL into a browser window if the link above does not work for you:
https://uwmadison.co1.qualtrics.com/jfe/form/SV_5hb8IoChRH0IVSK