UW-Madison
HIPAA Training

MAY 5, 2021

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

- You provide Business Associate Services to UW-Madison

This training course is estimated to require 15-20 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).
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 [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
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 subjects’ 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><strong>1.</strong> Names or Initials</td>
<td><strong>10.</strong> Account Numbers</td>
</tr>
<tr>
<td><strong>2.</strong> All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geographical codes</td>
<td><strong>11.</strong> Certificate/License Numbers</td>
</tr>
<tr>
<td><strong>3.</strong> 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>
<td><strong>12.</strong> Vehicle Identifiers and Serial Numbers, including License Plate Numbers</td>
</tr>
<tr>
<td><strong>4.</strong> Telephone Numbers</td>
<td><strong>13.</strong> Device Identifiers and Serial Numbers</td>
</tr>
<tr>
<td><strong>5.</strong> Fax Numbers</td>
<td><strong>14.</strong> Web Universal Resource Locators (URLs)</td>
</tr>
<tr>
<td><strong>6.</strong> Email Addresses</td>
<td><strong>15.</strong> Internet Protocol (IP) Address Numbers</td>
</tr>
<tr>
<td><strong>7.</strong> Social Security Numbers</td>
<td><strong>16.</strong> Biometric Identifiers, Including Finger and Voice Prints</td>
</tr>
<tr>
<td><strong>8.</strong> Medical Record numbers</td>
<td><strong>17.</strong> Full Face Photographic Images and Any Comparable Images</td>
</tr>
<tr>
<td><strong>9.</strong> Health Plan Beneficiary Numbers</td>
<td><strong>18.</strong> 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 and research data files – whether paper or electronic
- Research data sets which include direct identifiers
- Student coursework which includes direct 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 subjects 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 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.
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 [HIPAA Policy 3.8](#) for more information about this standard.
Handling and Distributing PHI

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 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.
De-identified Health Information

Data which has been de-identified no longer qualifies as PHI and is not subject to HIPAA. When you or trainees you supervise work with de-identified data, an individual’s authorization is not necessary prior to using or disclosing the PHI.

▪ **“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 the PHI 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](#) or the [HIPAA Privacy Officer](#) for more information.
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
- Elements of 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 (discussed later with New Resources).
HIPAA and UW-Madison policy allow certain email communications with PHI:

- Patients are 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 – among “wisc.edu” addresses or among wisc.edu and external email addresses within approved domains*. UW-Madison Health Sciences Students are trained to use their wisc.edu email accounts and not personal third-party accounts when they need to exchange PHI via email.

- External emails containing PHI must be encrypted.

See HIPAA Policy 8.6 for information about emailing PHI.

*Requires NetID Authentication
Email Communications Involving PHI

In addition to following UW-Madison’s 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 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
- Review your email lists and frequent contacts to ensure you direct email messages to the correct individuals
Maintaining patients’ and research subjects’ 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 UW-Madison 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.
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.
Storage and Computing Environments for PHI

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

▪ Access PHI from computers, mobile devices, and other tools maintained and/or managed by trained IT staff who support your unit of campus

▪ Use computing and data storage tools which are approved for use with PHI
Clinical or Research appointment details must be stored securely 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 Microsoft 365 calendars or other personal calendars (such as Google Calendars or iCal).

- At UW-Madison, our workforce is trained regarding the use of clinical schedule apps available through Epic called “Haiku” and “Canto.” If you supervise UW-Madison Health Sciences Students and want them to use certain approved secure apps, be sure you provide guidance about how to use them and any security settings you require them to configure on their mobile devices.
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” in which the Business Associate agree to use appropriate physical, technical, and administrative safeguards to protect PHI.

- UW-Madison’s Business Associate Agreement templates are available in the expandable Forms menu at this 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 this form (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 send research recruitment mailings)
- Third-party Claims Administrators
Business Associates

Business Associate Agreements (BAAs) may be reviewed by the following offices at UW-Madison:

- Office of Research and Sponsored Programs
- UW-Madison Procurement
- Office of Compliance - HIPAA Privacy Officer
- SMPH Contracting Office

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

- When related to research projects, route BAAs via WISPER with other project documents

- BAAs must be executed by individuals with Board of Regents signature authority (see the Signature Authority Memo at this link)

- See HIPAA Policy 6.1 for details about engaging Business Associates for UW-Madison

- See HIPAA Policy 6.2 for information about providing Business Associate services for another Covered Entity
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)

- DUA templates and review of DUAs may be requested from any of the following:
  - Office of Research and Sponsored Programs
  - UW-Madison Procurement
  - Office of Compliance - HIPAA Privacy Officer
  - SMPH Contracting Office

- **Using approved DUA templates will reduce DUA review and execution timelines!**

- When related to research projects, route DUAs via WISPER with other project documents

- DUAs must be executed by individuals with Board of Regents signature authority (see the Signature Authority Memo at [this link](#))

- See [HIPAA Policy 5.2](#) for details about LDSs of PHI and DUAs
New Resources to support HIPAA Compliance at UW-Madison
In connection with the UW-Madison Policy Library Project, all HIPAA policies are now stored centrally in the Policy Library at policy.wisc.edu.

- This is a single-up-to-date resource for all official university-wide policies.
- Update policy bookmarks as needed in your school, college, or division webpages.
- Locate UW-Madison HIPAA Policies through either the Office of Compliance HIPAA website or the Policy Library – both channels point to the same policy content.
A list of approved tools for use with PHI was first published in March of 2020, and is updated periodically to add or remove tools as needed.
Reminder: Tools NOT Approved for Use with PHI

At UW-Madison, the following products are not approved for use with PHI. The use of these tools with PHI at UW-Madison should be reported using the online HIPAA Incident Report Form discussed in the following slides:

- Google Suite (G-Suite) Tools – including Gmail, GoogleCalendar, GoogleDocs, GoogleSheets
- Canvas – do not upload course assignments with PHI
- ZendTo
- Personal Email Accounts
- Personal File-sharing Accounts (DropBox, GoogleDrive, OneNote)
- Social Media (Facebook, Twitter, Instagram, Snapchat) or their Messaging Tools
A new illustration was created to show the roles, committees, and offices that support HIPAA compliance at UW-Madison (available at compliance.wisc.edu/hipaa)
New guidance was published this past year to address common questions about sharing Human Subjects research data.
New guidance was also published recently to address common questions about receiving Human Subjects research data from external entities.
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! (This is especially true when an incident involves suspected IT security vulnerabilities or theft of a mobile device.)
- UW-Madison’s HIPAA Incident Report Form is 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:

- Access by a student or trainee to records which they should not have reviewed in connection with a clinical rotation
- IT vulnerabilities caused by phishing, hacking, failure to update operating systems or applications, or incorrect configuration of website settings
- Loss or theft of an individual’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 (such as receiving a data set from a researcher which included dates, despite the researcher intending to send de-identified data)
- Suspected password-sharing or compromised usernames/passwords
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, call or email the UW-Madison HIPAA Privacy Officer:

Amanda K. Reese, JD, CHPC, CPHRM
amanda.reese@wisc.edu
608-262-2059
Reminder: HIPAA Resources & Support

This training will remain accessible until the release of the next HIPAA training course during the 2021-2022 academic year.

▪ Refer to the training as needed to answer your HIPAA compliance questions

▪ Contact the HIPAA Privacy Officer, the HIPAA Security Officer, or your HIPAA Privacy or Security Coordinators for assistance navigating a specific HIPAA-related matter
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_9sODr71K6ENT60m