UW-Madison

HIPAA Privacy & Security Training 2019-2020

(***Public-facing Training Which Does Not Require a UW-Madison NetID***)

UW-Madison Office of Compliance

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 are a Business Associate of UW-Madison.

This training course is estimated to require 20-25 minutes to complete, and does not contain audio.

With technical questions, please contact help@doit.wisc.edu or call 608-264-HELP (608-264-4357).

Before we begin… Why do I take this?

And if I've taken it before, why do I have to take this every year?

In accordance with HIPAA, UW-Madison's HIPAA Training Policy requires that training be provided to members of the UW-Madison HIPAA-covered "workforce" before gaining access to protected health information and on an annual basis thereafter. Even workforce members who do not routinely work with protected health information are trained annually to satisfy regulatory requirements and comply with UW-Madison's HIPAA Training Policy.

This training:

- Reinforces HIPAA privacy and security topics covered in previous trainings and reminders
- Provides information about where to report HIPAA incidents online, where to find HIPAA-related news, and where to find resources for additional guidance

As always: Contact UW-Madison's HIPAA Privacy or Security Officers or a HIPAA Privacy or Security Coordinator with questions.

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

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).

It applies to:

- Individual healthcare providers (like physicians, nurses, pharmacists)
- Institutional providers (such as hospitals and health systems)
- All forms of Protected Health Information ("PHI" – described in more detail later), including paper, electronic, verbal, and visual
- Human subjects researchers working with PHI

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

OCR's HIPAA resources are available at: http://www.hhs.gov/ocr/privacy/index.html

When you need information about HIPAA at UW-Madison, visit www.compliance.wisc.edu/hipaa.

How does HIPAA apply to UW-Madison?

UW-Madison is an institutional healthcare provider subject to HIPAA.

- It is a "hybrid entity" for HIPAA compliance purposes – 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 UW-Madison HIPAA Policy 1.1 for a detailed listing of the areas of campus included in the UW HCC.

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

Members of UW-Madison and individuals external to UW-Madison become part of the UW HCC when they perform functions with or for the UW HCC such as:

- Working on research studies
- Collaborating on quality improvement projects
- Volunteering or serving as a preceptor for a unit of the UW HCC (including zero-dollar appointees)

How does HIPAA apply to UW-Madison?

Compliance with UW-Madison HIPAA policies is required of all members of the workforce of the UW HCC.

The UW HCC is trusted to safeguard PHI. It is critical that the UW HCC workforce protect the privacy and security of our patients' and our research subjects' PHI. It's the law, and it's the right thing to do.

Remember: Compliance with HIPAA is the collective responsibility of all of us.

We need to be good stewards of our patients' and research subjects' information.

This is required by law(s), helps us avoid fines, and is the right thing to do!

What are the consequences of not complying with HIPAA?

Failing to comply with HIPAA May lead to legal and professional consequences:

- Unintentional disclosures of PHI and unintentional violations of HIPAA often involve **correction action plans and fines** imposed by the federal government.
- Intentional violations of HIPAA may lead to **criminal proceedings and jail time**.
- At UW-Madison, unauthorized access to PHI may result in **termination of employment** (for employees), **removal from a clinical rotation or expulsion** (for students), or **removal of access to PHI** (for employees, students, collaborators, business associates).

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, and **decreases the likelihood that they will authorize use of their information for research purposes**.

What is PHI?

PHI stands for "**Protected Health Information**." which is any individually-identifiable health information ***created*** or ***received*** by a health care provider relating to the past, present or future:

- physical or mental health conditions of the individual, or
- The provision of health care to the individual, or
- 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 written, electronic, verbal, or visual.

18 HIPAA Identifiers

1. Names or Initials
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes
3. All elements of dates (except year) for dates directly related to an individual, *including*
    a. birth date
    b. admission date
    c. discharge date
    d. date of death
    e. *and* all ages over 89 and all elements of dates (including year) indicative of such age (they may be aggregated into a single category of “age 90 or older”)
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Any unique account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) addresses
16. Biometric identifiers, including fingerprints and voiceprints
17. Full-face photos and comparable images
18. Other unique identifying numbers, characteristics, or codes, unless permitted by HIPAA.

Examples of PHI

PHI can be in paper, electronic, digital, verbal, or visual forms – such as:

- 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
- Clinical or research appointment schedules
- Emails sent to/from patients or potential research subjects about their health-related conditions or questions
- MRI scan data
- Videos or photos taken during physical therapy / gait-assessment sessions
- Individually-identifiable photos and videos of patients or research subjects at certain events (Learn more about HIPAA compliance when interacting with the media or the public at this link)

Using and Disclosing PHI:

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

- Treatment
- Payment
- Health Care Operations

Researchers may also use PHI without authorization or with a waiver of HIPAA's authorization requirement for limited "preparatory to research activities."

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

Researchers may also use and share PHI in accordance with authorization or a waiver (or alteration) of HIPAA's authorization requirement as approved by an IRB or Privacy Board.

Minimum Necessary Standard

When you use or share PHI for payment or health care operations purposes, you are required to use and disclose only the minimum amount of PHI necessary to accomplish your intended purpose. Health care operations include administrative, financial, legal, and quality improvement activities necessary to conduct healthcare business and support the core functions of treatment and payment.

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:

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

Please refer to UW HIPAA Policy 3.8, The Minimum Necessary Standard for more information.

Using and Disclosing PHI – Special Circumstances:

For **media or promotional uses of PHI** (such as social media posts, journal articles, news stories, or documentaries) written authorization from the patient or research subject involved must be obtained in advance. Authorization forms are available at the HIPAA Compliance webpage (compliance.wisc.edu/policies-and-forms/).

Additionally, if news media is involved, be sure to contact the UW-Madison HIPAA Privacy Officer or UW Health's Media Relations team (if UW Health facilities are involved). Those individuals will ensure appropriate review and involvement of all stakeholders.

HIPAA permits (but does not mandate) certain other disclosures of PHI for activities such as **public health** activities, **workers' compensation**, and specialized **government functions** without first obtaining an individual's authorization to do so. Those situations are too specific to detail in this basic training. If you have questions about a specific situation, contact the UW-Madison HIPAA Privacy Officer.

Accessing PHI in Electronic Systems

UW-Madison grants role-based access to electronic systems containing PHI (such as Secure Box Folders or REDCap databases). This means access is permitted only if your role requires you to have access to PHI in order to perform the functions of your role.

If you need role-based electronic access to PHI, you will receive a username and password for such access. You may ONLY access PHI to perform the functions of your job.

- NEVER attempt to gain access to electronic PHI through other means (such as "borrowing" the user name and password of another individual).

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

- A current or former relative (including a child, a spouse or ex-spouse, or any other family member)
- A friend, neighbor, co-worker, or acquaintance
- A celebrity, public figure, or someone you learn about in news media (such as political figures, community leaders, individuals involved in accidents reported in the news, etc.)

Your own curiosity or desire to learn about a particular health condition is not a legitimate educational reason to access the PHI of a patient or research subject. If you have questions about this, contact the HIPAA Privacy Officer.

Unauthorized access to PHI may result in discipline up to and including

termination of your employment (for employees),

termination of your collaboration or affiliation with UW-Madison (for volunteers, preceptors, etc.) and

removal from a clinical rotation or expulsion (for students).

Audits of Electronic Access to PHI

Any inappropriate access to individuals' records may result in an audit and investigation and possible corrective action. Depending on the circumstances of access, you could **jeopardize your affiliation with UW-Madison or your participation in educational programming** if you inappropriately access PHI.

If you are ever uncertain about whether you can access certain PHI, seek guidance from one of these resources:

- The UW-Madison HIPAA Privacy Officer
- Your UW-Madison HIPAA Privacy Coordinator

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

- Use strong passwords
- Never write out your passwords and save them on a sticky note on your computer screen or under a keyboard
- Log out of your computer or lock your workstation when you leave your workstation
- Never share your passwords with anyone

Handling and Distributing PHI

In addition to accessing PHI appropriately and with the Minimum Necessary Standard in mind, we must be careful when sharing PHI.

When you handle hard-copy PHI (such as appointment summaries, completed research questionnaires, etc.), **double-check to make sure you hand or mail the information to the correct person**.

Be conscious of the paperwork you carry with you to **avoid inadvertently leaving PHI 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 the individual/company first to confirm the number.

Safeguarding PHI

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

Several ways you can do this include:

- Limiting your risk by working with de-identified information or Limited Data Sets
- Accessing PHI in accordance with the “Minimum Necessary” Standard
- Paying attention to detail when Using and Disclosing/Sharing PHI
- Accessing PHI from secure/updated/patched workstations and devices

De-identification of PHI

Data which has been de-identified no longer qualifies as PHI and is not subject to HIPAA.

- De-identification can be accomplished by removing the 18 HIPAA identifiers (listed earlier) from the information you need to work with.
- Removing all of these identifiers can be challenging.
- Layering several unique data elements (such as athlete status and sport played, a genetic condition, a specific type of occupation or injury) may result in the information still being deemed identifiable.

For assistance with de-identification, contact a HIPAA Privacy Coordinator or work with the ICTR Clinical Research Data Service. See UW-Madison HIPAA Policy 5.1 for more information about de-identification.

Data is *NOT* de-identified if it includes dates (dates of service, dates of birth, dates of death), initials, zip codes, medical record numbers, GPS data, IP addresses, or biometric identifiers.

Email

We frequently use email to send PHI to other health care providers, instructors, research colleagues, and administrators. The HIPAA Privacy Rule permits using and disclosing PHI this way – but requires us to use appropriate safeguards to protect the privacy of the PHI.

***Before emailing PHI*, consider whether better methods exist for sharing the PHI involved.**

- UW-Madison can establish Secured Box Folders to facilitate sharing of PHI for UW-Madison purposes (such as for sharing PHI with external research collaborators).
- Secured Box Folders must be requested using this process.
- Google Products should *NOT* be used at UW-Madison to create, store, or share PHI. (This includes Gmail, GoogleDrive, GoogleCalendar, and GooglePhotos).

Electronic Calendars

Clinical or research appointment details should be stored securely only in appropriate/approved tools such as electronic medical records systems or other institutionally-endorsed data storage or scheduling systems.

Do not copy-and-paste PHI from medical records or research files into electronic calendars. Doing so jeopardizes the privacy, security, and confidentiality of the PHI.

This is especially true when calendars are shared with other individuals (who may not be approved for access to the PHI), when calendars sync to mobile devices, or when the calendars are cloud-based products of vendors with which UW-Madison does not have a Business Associate Agreement. In these cases, including PHI in your electronic calendars can result in unauthorized disclosures of PHI and HIPAA breaches.

Additional Information for Researchers

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

Research resources are available on the HIPAA Compliance website at https://compliance.wisc.edu/hipaa/researchers/.

Please note that Human Subjects Research regulations (the "Common Rule") and HIPAA have different requirements.

When a research study is exempt from IRB review under the Common Rule, HIPAA still applies.

Business Associates / Business Associate Agreements

Individuals and businesses that provide services for UW-Madison which involve the use or storage of PHI on behalf of UW-Madison are "Business Associates." Before doing business with them, UW-Madison requires them to enter into "Business Associate Agreements" in which they agree to use appropriate physical, technical, and administrative safeguards to protect UW-Madison's PHI.

Business Associates include:

- cloud-based service providers
- shredding vendors
- media sanitization vendors
- eFax solution providers
- transcriptionists (such as those who transcribe research interviews)

Google products are NOT currently approved for storage of PHI at UW-Madison.

At UW-Madison, PHI may not be stored in or shared with others using Google products. This includes Gmail, GoogleDrive, GoogleCalendar, and GooglePhotos.

If you become aware of UW-Madison patients' or research subjects' PHI being stored in or shared via Google Products, please report the incident using the online HIPAA Incident Report Form discussed in the following slides.

Incident Reporting

Unfortunately, accidents and mistakes with PHI happen… Any time you suspect that an incident involving the **loss**, **theft**, or **misdirection of PHI** has occurred which involves UW-Madison, you should **immediately** complete a UW-Madison HIPAA Incident Report Form so the incident can be investigated and addressed promptly.

UW-Madison's HIPAA Incident Report Form is available online at the HIPAA Compliance website.

Federal regulations require UW-Madison to investigate and document the investigation of all HIPAA Incidents, and might also require notifications (to the affected individuals, news media, and OCR) within a specific timeline.

If you have questions about a possible HIPAA Incident that you'd like to talk through before submitting an online HIPAA Incident Report Form, please take one or more of the following actions:

- Call oremail the UW-Madison HIPAA Privacy Officer
- For research-related incidents, call the UW-Madison's anonymous Human Research Protection Program Hotline at 608-890-1273

The UW-Madison HIPAA Incident Report Form looks like this:

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

HIPAA Incident Report Form

Reporter Information

List your contact information:

First and Last Name

Title

UW-Madison Resources:

Please access additional resources as needed at the hyperlinks below

- HIPAA Policies
- Research Forms (Registrations and Certifications)
- Contract Templates & Authorizations
- HIPAA Incident Report Form
- HIPAA Security Resources
- HIPAA Privacy Officer, HIPAA Security Officer, HIPAA Privacy & Security Coordinators

Remember: Compliance with HIPAA is the collective responsibility of all of us.

Thank you for being good stewards of our patients' and research subjects' information.

This is required by law(s), helps us avoid fines, and is the right thing to do!

You are almost done...

Click here to provide basic contact information to UW-Madison, and to verify your understanding of this training.

We will forward proof of completion of this training to your preferred email address.

Thank you.