UW-Madison and UW Health Approved Tools for
Exchanging and/or Storing Protected Health Information (PHI)

December 20, 2023

This reference is intended to facilitate the use of approved tools for exchanging, capturing, analyzing, and/or storing the Protected Health Information (PHI) of patients and research subjects in accordance with HIPAA.

These tools are expected to be used by employees, students, and other agents of UW Health and UW-Madison – with computers and devices issued or managed by UW Health or UW-Madison.

Neither UW Health nor UW-Madison approves the use of these tools to facilitate working with PHI on personally-owned and/or unmanaged computers or devices, except when specifically permitted by policy or procedure.

Please direct any questions regarding intended use of these tools or options for approved remote access to the UW Health Security Team (via UW Health's Service Desk at 265-7777), or to UW-Madison HIPAA Security Coordinators as needed for clarification.

Please contact the relevant Help Desk if you have questions about how to configure, implement or use any of these tools.

This reference will be updated periodically to add or remove tools as appropriate.

1. APPROVED

1.1 Tools Licensed by UW Health

1.1.1 Health Link
1.1.2 Health Link InBasket Messaging
1.1.3 Epic Haiku (iOS or Android) and Epic Canto (for iPads)
1.1.4 Epic Secure Chat
1.1.5 MyChart (Ambulatory)
1.1.6 MyChart Bedside (Inpatient)
1.1.7 Cisco Webex (Meetings and Chat)
1.1.8 SharePoint
1.1.9 uwhealth.org or uConnect Website Forms
1.1.10 For delivery of UW Health Clinical Telehealth Services to Patients, MyChart Video Visits, Vidyo, AmWell, and WebEx (limited cases)*
1.1.11 For other calls, VoIP Phone Services used with devices provided or managed by UW Health or UW-Madison

** Staff who provide telehealth services at UW Health or any other healthcare facility must follow the policies and guidance for provision of telehealth to patients at each facility.*

1.2 Tools Licensed by UW-Madison

1.2.1 Phone calls using UW-Madison:
1.2.1.1 provided landlines or VoIP services
1.2.1.2 provided or managed mobile device
1.2.1.3 approved call applications e.g., Cisco jabber (Deprecated. It is being replaced by Cisco Webex), Microsoft Teams, Cisco Webex, Secure Zoom^
1.2.2 Globus^^
1.2.3 Microsoft Teams
1.2.4 Qualtrics
1.2.5 Research Drive^^
1.2.6 Secure Box Folders^^ (Not standard-issue Box Folders)
1.2.7 Cisco Webex Meetings & Webex Teams
1.2.8 Secure Zoom (To confirm enrollment in SecureZoom see https://kb.wisc.edu/112923)
1.2.9 UHS and Athletics electronic medical record systems
1.2.10 Platform X
1.2.11 Enterprise Content Management Service (ECMS) Imaging

^ *Determine if you are enrolled in secure Zoom at https://kb.wisc.edu/zoom/page.php?id=113688#difference*
^^ *Request use at go.wisc.edu/hipaasecurity*

1.3 Tools Made Available to UW Health or UW-Madison by Third Parties

1.3.1 Sponsor or collaborator provided Databases or Portals for Research Data
1.3.2 Databases provided for Data Registry Participation

2. USE WITH CAUTION

2.1 Tools Licensed by UW-Madison

2.1.1 REDCap instances that have been risk assessed by the Office of Cybersecurity

2.1.2 SharePoint Online (See https://kb.wisc.edu/office365/page.php?id=75636)

2.1.3 Google Cloud Platform (Request use via the UW-Madison Public Cloud Team at cloud-services@cio.wisc.edu)

2.1.4 Amazon Web Service (AWS) (Request use via the UW-Madison Public Cloud Team at cloud-services@cio.wisc.edu)

2.1.5 Microsoft Office 365 work-issued email *(generally ending in wisc.edu)*

*** Do not place patient/subject name, MRN, study ID in subject line*

*** Use lower-risk identifiers in message body (i.e., MRN and DOB or initials instead of full names)*

*** Use Office Message Encryption if emailing externally*

*** Use caution when attaching documents*

*** Be sure you know what ePHI is in any document you email, and that the recipients are authorized to receive the ePHI*

*** Consider approved file-sharing/collaboration tools listed above instead of email rather than attaching reports or data sets containing ePHI to email*

*** In the research context, follow IRB Email Guidance: https://irb.wisc.edu/manual/investigator-manual/conducting-human-participant-research/recruitment-guidelines/?tab=email-recruitment-guidelines*

*** Patients should be encouraged to interact with healthcare providers through patient portals*

*** If patients email healthcare providers directly, they should first be redirected to patient portals. If patients insist on communicating through email, they must be advised of risks of emailing PHI*

*** At UW-Madison, if you require "mail list" functionality for messages that include PHI, use Office 365 Groups instead of GoogleGroups*

2.1.6 CloudFax enables both inbound and outbound faxing using an email based workflow

** To learn more see https://it.wisc.edu/services/cloudfax/*

2.1.7 Institutional Shared Network Drives

** Should not be used to store duplicative or "shadow" copies of Health Link or Enterprise Data Warehouse data*

2.2 Tools Licensed by UW Health

2.2.1 UW Health's internal web paging system

2.2.2 Well SMS/Text Messaging platform which uses automated protocols for one-directional communication

** Patients or family members must opt in

** Patients or family members must not be able to respond

** Must be approved by UW Health Privacy Officer on a case-by-case basis

2.2.3 Institutional Shared Network Drives

** Should not be used to store duplicative or "shadow" copies of Health Link or Enterprise Data Warehouse data

**Store sensitive and restricted data types in a "SpecialShares" folder with limited permissions.

2.2.4 Microsoft Office 365 work issued email (generally ending in uwhealth.org)

**Reference UW Health policy on using email to send sensitive or restricted data, P&P

6.31, available on UConnect: E-Mail Transmission of Sensitive or Restricted Data - Policy Number: 6.31 (wisc.edu)

2.2.5 RightFax enables inbound and outbound faxing using the RightFax application. Some outbound workflows are integrated with other applications, like Health Link, to facilitate electronic signatures on documents.

** *To learn more or convert a physical fax machine to a RightFax queue, contact the UW Health help desk at 265-7777*

** *Verify fax number*

** *Use Cover Sheet*

** *Only use institutionally-provided vendors and institutionally-provided fax equipment*

** *Do not use other electronic fax services like Doximity, eFax or other services*

3. DO NOT USE / NOT APPROVED / NOT PERMITTED

If you become aware any of the following tools are or have been used with PHI, submit a HIPAA Incident report as soon as possible to UW Health or to UW-Madison.

3.1. Personally acquired software or tools (eg: email accounts, file-sharing accounts, and instant messaging accounts)

3.2. Microsoft Office 365 – Calendar Entries with PHI

3.3. Canvas (UW-Madison's Web-based Course Delivery Platform)

3.4. G-Suite/Workspace (Google) Tools (Gmail, Drive, Docs, Sheets, Slides, Forms, Calendar, Google+, Hangouts)

3.5. Social Media (Facebook, Twitter, Instagram, Snapchat)

***In some situations, an IRB may approve a research protocol involving the use of social media; if so, social media may only be used as stated in the approved protocol*

3.6. Other Organizations' Text or Web Paging Systems (Text pages should not include patient/subject identifiers)

3.7. Texting

***In some situations, an IRB may approve a research protocol involving the use of texting; if so, texting may only occur as stated in the approved protocol*

3.8. Virtual Assistants (Alexa, Echo Dot, Siri, Bixby, Alice)

3.9. VoIP Phone Services not provided by UW Health or UW-Madison (Google Voice, WhatsApp)

3.10. Other Apps, Software, Tools from Cloud Service Providers (e.g.: Slack, and ZendTo) *not reviewed and approved by UW Health or UW-Madison*

To propose a tool for inclusion in the "Approved" or "Use with Caution" sections of this resource, please contact:

UW Health: privacyofficer@uwhealth.org
UW-Madison: hipaa@wisc.edu

[*See Following Pages for References*]

Relevant Supporting References

A. UW Health Policies

1. Policy 6.31, E-Mail Transmission of Protected Health Information
2. Policy 6.32, Provider-Patient Email
3. Policy 1.01, Remote Access to Electronic Information Systems
4. Policy 1.46, UW Health Mobile Device Policy
5. Policy 1.29, Computer, Electronic, Communication and Internet Usage via UW Health Resources
6. Policy 1.54, Appropriate use of UW Health Chat, Paging, Instant Messaging, and Text Messaging Technologies

B. UW-Madison HIPAA Policies

1. HIPAA Policy 8.5, Security of Faxed, Printed and Copied Documents Containing PHI
2. HIPAA Policy 8.6, E-mail Communications Involving Protected Health Information

C. UW-Madison Guidance & Resources

1. UW-Madison HIPAA Privacy / Office of Compliance
2. UW-Madison HIPAA Security / Office of Cybersecurity
3. Health Sciences IRB, Use of Email for Research Purposes
4. Safe Computing When Traveling Abroad

D. United States Dept of Health & Human Services Office for Civil Rights Guidance

1. Guidance on HIPAA and Cloud Computing

V1: March 20, 2020
V2: March 26, 2020
V3: February 9, 2021
V4: February 19,2021
V5: April 13, 2022
V6: December 20, 2023