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

February 9, 2021

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 Consultant Security Team (via UW Health’s Help Desk at 265-7777), or to UW-Madison HIPAA Security Coordinators as needed for clarification.

NOTE FOR COVID-19: During the COVID pandemic, some accommodations have been made to allow for remote work, research, and instruction. With world-wide shortages of equipment, some may be using personal devices or tools not otherwise permitted by applicable policies. These accommodations should not be considered permanent and will be re-evaluated when possible.

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

1.1 **Voice Calling**
   1.1.1 Phone Calls using standard landlines or cellular services
   1.1.2 VoIP Phone Services used with devices provided or managed by UW Health or UW-Madison

1.2 **Tools Licensed by UW Health**
   1.2.1 Health Link
   1.2.2 Health Link InBasket Messaging
   1.2.3 Epic Haiku (iOS or Android) and Epic Canto (for iPads)
   1.2.4 Epic Secure Chat
   1.2.5 MyChart (Ambulatory)
   1.2.6 MyChart Bedside (Inpatient)
   1.2.7 Cisco Webex and Cisco Teams
   1.2.8 SharePoint
   1.2.9 uwhealth.org or uConnect Website Forms
   1.2.10 For delivery of UW Health Telehealth Services to Patients: Vidyo, AmWell, and WebEx (limited cases)*

   * 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.

1.3 **Tools Licensed by UW-Madison**
   1.3.1 Globus
   1.3.2 Microsoft Teams
   1.3.3 Qualtrics
   1.3.4 REDCap
   1.3.5 Research Drive
   1.3.6 Secure Box Folders (Not standard-issue Box Folders)
   1.3.7 SharePoint Online (the instance supported by DoIT)
   1.3.8 Cisco Webex Meetings & Webex Teams

   ^^ Request use of Globus, Research Drive, or Secure Box at go.wisc.edu/hipaasecurity

1.4 **Tools Made Available to UW Health or UW-Madison by Third Parties**
   1.4.1 Sponsor-provided Databases or Portals for Research Data
   1.4.2 Databases provided for Data Registry Participation
2. USE WITH CAUTION

2.1 Microsoft Office 365 Email provided by UW Health or UW-Madison
** Use ONLY work-issued email address (generally ending in uwhealth.org or 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. For example, rather than attaching reports or data sets containing ePHI to email, deliver them via secure file-sharing options such as SharePoint, Secure Box Folders, Globus, etc.
** In the research context, follow IRB Email Guidance: https://kb.wisc.edu/hsirbs/71745
** 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

2.2 Electronic Fax Services provided by UW Health (RightFax) or UW-Madison (CloudFax)
2.2.1 UW Health: 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
2.2.2 UW-Madison: CloudFax enables both inbound and outbound faxing using an email based workflow
** To learn more see https://it.wisc.edu/services/cloudfax/

2.3 Institutional Shared Network Drives provided by UW Health or UW-Madison
** Should not be used to store duplicative or “shadow” copies of Health Link or Enterprise Data Warehouse data

2.4 Tools Licensed by UW Health
2.4.1 Cisco Jabber IM (Internal) – deprecated. It is being replaced by Cisco Teams.
2.4.2 UW Health’s internal web paging system
2.4.3 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
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 **Personal Email Accounts**
3.1. **Personal File-sharing Accounts** (DropBox, GoogleDrive, OneNote)
3.2 **Personal Instant Messaging Accounts**
3.3 **Microsoft Office 365 – Calendar Entries with PHI**
3.4 **Amazon Web Service (AWS)**
3.5 **Canvas** (UW-Madison’s Web-based Course Delivery Platform)
3.6 **Google Cloud Platform**
3.7 **G-Suite (Google) Tools** (Gmail, Drive, Docs, Sheets, Slides, Forms, Calendar, Google+, Hangouts)
3.8 **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**
3.9 **Other Organizations’ Text or Web Paging Systems** (Text pages should not include patient/subject identifiers)
3.10 **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**
3.11 **Virtual Assistants** (Alexa, Echo Dot, Siri, Bixby, Alice)
3.12 **VoIP Phone Services not provided by UW Health or UW-Madison** (Google Voice, WhatsApp)
3.13 **ZendTo**
3.14 **Zoom** (Except for the approved use of Zoom at UW-Madison’s University Health Services clinic)
3.15 **Other Apps, Software, Tools from Cloud Service Providers unless reviewed and approved by UW Health or UW-Madison, as appropriate**

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

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
This reference was created through collaborative efforts of a task force established by UW Health and UW-Madison in August of 2018 to review electronic tools used with protected health information.

The group formally completed its charge and disbanded – and the initial list of tools approved for use with PHI continues to be updated with input from UW Health’s and UW-Madison’s HIPAA Privacy and Security Officers, IT leadership, and legal counsel.

Initial Membership of the Task Force appears below:

**Executive Sponsors:**
- Elizabeth Burnside, MD; SMPH Deputy Exec. Director of ICTR
- Jocelyn DeWitt, PhD; UW Health Senior Vice President, Chief Information Officer

**Co-Chairs:**
- Troy Lepien, MAB, CIA, CHC, CHPC; UW Health Vice President of Business Integrity and HIPAA Privacy Officer
- Amanda Reese, JD, CHPC, CPHRM; UW-Madison HIPAA Privacy Officer
- Ryan Moze, JD; SMPH HIPAA Privacy Coordinator

**Members:**
- Shannon Dean, MD; UW Health Sr. Vice President and Chief Medical Information Officer
- Paul VanAmerongen; UW Health Vice President and Chief Information Security Officer
- Joel Buchanan, MD
- Robert Lemanske, MD
- Rebecca Marnocha, PharmD; SMPH Director of Clinical Research and Assoc. Exec. Director of ICTR
- Claire Dalle Molle, JD; UW-Madison University Legal Counsel
- Richard Konopacki; SMPH IT Director and HIPAA Security Coordinator
- Rebecca Rankin; UW Health Director of Nursing Informatics
- Hope Thompson, CHP, CHPC; SwedishAmerican HIPAA Privacy Officer
- Stefan Wahe, CISSP; UW-Madison Assoc. Chief Information Security Officer and HIPAA Security Officer
- Lisa Wilson, JD; UW-Madison Senior University Legal Counsel