Email Communications Involving Protected Health Information

Effective Date: March 14, 2004
Last Updated: March 26, 2020
Previously Updated: November 11, 2019, June 3, 2015

Policy Summary

The University of Wisconsin-Madison is committed to maintaining the privacy, confidentiality and security of patients’ and research subjects’ protected health information (“PHI,” defined below). This policy sets forth requirements and safeguards which must be undertaken when UW-Madison faculty and staff use e-mail to transmit PHI.

UW-Madison protects and safeguards PHI when communicating via e-mail to prevent access by unauthorized individuals or entities. External e-mail communication containing PHI must be encrypted wherever possible, and also noted in medical records when relating to clinical treatment, recommendations or follow-up. Further, where encryption is not used, UW-Madison faculty and staff must inform patients and research subjects about the risks of communicating PHI through unsecured e-mail, and must take reasonable measures to safeguard the content and transmission of such e-mail.

UW-Madison encourages faculty and staff, before communicating PHI via email, to consider whether a better method exists for communication of the information. More-secure alternatives might include utilizing messaging tools available within an Electronic Medical Record system, utilizing collaboration tools endorsed by UW-Madison Cybersecurity, or sharing information through folders in local network drives. Faculty and staff should consult with the UW HIPAA Security Coordinator for their unit of campus with questions about secure alternatives.

UW-Madison strictly prohibits the email transmission of HIV test results and/or treatment records information involving mental health care or alcohol or drug addiction.

Who This Policy Applies To

Applies to all members of the UW-Madison Health Care Component.

Rationale

In enacting HIPAA, Congress mandated the establishment of Federal standards for the privacy of individually identifiable health information. Under the patchwork of laws existing prior to adoption of HIPAA and the Privacy
Rule, personal health information could be distributed—without either notice or authorization—for reasons that had nothing to do with a patient’s medical treatment or health care reimbursement. For example, unless otherwise forbidden by State or local law, without the Privacy Rule patient information held by a health plan could, without the patient’s permission, be passed on to a lender who could then deny the patient’s application for a home mortgage or a credit card, or to an employer who could use it in personnel decisions. The Privacy Rule establishes a Federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections apply over and above the new Federal privacy standards.

Policy Detail

1. Communicating with Patients by E-mail

1.1 Health care providers may not send External Email to patients via email except according to the specific standards set forth in this policy. Providers are encouraged to use other secure means of communication first. Similarly, patients should be encouraged to use patient portals provided by their health care providers for sending secure electronic communications to their providers. This ensures that such communications are secure, addressed in a timely fashion, and appropriately documented within the appropriate electronic health record.

Commonly used patient portals in the Madison, Wisconsin, area include:

- uwhealthmychart.org (for UW Health)
- myuhs.uhs.wisc.edu (for University Health Service)
- chart.myunitypoint.org (for UnityPoint Health-Meriter)
- myhealth.va.gov/ (for the VA – Veterans Affairs)
- ghcscw.com/ghcmychart#/ (for Group Health Cooperative of South-central Wisconsin)

1.2 If a patient initiates e-mail correspondence with a health care provider, the health care provider shall encourage the use of a patient portal as described above. If a patient refuses to utilize a patient portal, before corresponding directly with a patient by e-mail, both the patient and the health care provider must agree to the use of e-mail as a form of communication and agree upon appropriate limits on the use of e-mail to facilitate their communication. The UW health care provider must explain the security risks involved with communicating PHI using e-mail, and may do so using the text provided in the following section.

1.3 Language in substantially similar form to that below should be added to a health care provider’s e-mail signature line to remind the patient of the security limitations of e-mail:

NOTICE TO PATIENTS: E-mail communications are not considered to be private or secure. There are many ways that both authorized and unauthorized users may have access to e-mail communications. Patients are strongly cautioned against sending sensitive, detailed personal information to providers via e-mail. E-mail should also not be used to convey information of an urgent nature. For urgent matters, patients should call their provider’s clinic.

1.4 Standards for E-mail Communications with Patients

1.4.1 Criteria for Use. Any health care provider wishing to communicate via e-mail with patients must establish criteria for determining when to use e-mail as a method of communication with patients. Such criteria should include a consideration of the health care provider’s patient base, including those patients’ unique needs, physical limitations, and communication style. The criteria should balance the need for ease and
efficiency of communication and the consequent delivery of health care against the need for examination of the patient and/or face-to-face communication, the documentation needs for billing compliance purposes, and the triaging capabilities available through e-Visit and Video-Visit technology.

1.4.2  Response Time. Each health care provider who uses email to communicate with patients must establish a standard response time for a material response to be sent to the patient. In no event may this standard exceed three (3) business days. In the event that a material response is not reasonably possible within this time period, an e-mail must be sent to the patient acknowledging receipt of the patient’s e-mail and informing the patient of:

- 1.4.2.1 The reason a response is not forthcoming within the standard time period;
- 1.4.2.2 When a material response may be expected; or
- 1.4.2.3 Advising the patient on a preferred/alternative method of communication and/or treatment delivery.

1.4.3  Out of Office. When a health care provider who has agreed to receive e-mails from patients is away from the office (conference, vacation, etc.) an auto-reply must be set in advance which notifies all correspondents that the health care provider is not available to answer e-mail.

2.  Communicating with Research Subjects by E-mail

2.1 All communications with Research Subjects must occur in accordance with UW-Madison Health Sciences Institutional Review Board Guidance on the ‘Use of Email For Research Purposes’ and with any approved research protocol applicable to the involved research.


3.  Communicating PHI to Any Party by E-mail Inside “wisc.edu” or Inside of the UW ACE

3.1 E-mail containing PHI may be sent internally to addresses which end in “wisc.edu.” Additionally, External Email containing PHI may be sent to email addresses within domains controlled by the UW ACE. These email messages do not require the senders or recipients to apply additional security controls in order for the messages to be deemed secure. Contact the HIPAA Privacy or Security Officers with questions about which domains are currently controlled by the UW ACE.

3.2  Electronic Storage. UW-Madison faculty, staff and students who store e-mail messages containing PHI may only do so using storage solutions managed and/or approved by UW-Madison or UW Health for storage of PHI. Contact your HIPAA Security Coordinator or submit a “Joint Security & Privacy Review Request” (“JSPR Request”) for assistance with secure storage solutions. JSPR Requests may be submitted electronically using the form available at go.wisc.edu/hipaasecurity.

4.  Communicating PHI by E-mail Outside of the UW ACE or the UW HCC

4.1 E-mail containing PHI sent to domains outside of the control of the UW ACE or the UW HCC must be encrypted. Contact your HIPAA Security Coordinator with questions about e-mail encryption.
5. General Security

5.1 UW-Madison E-mail Addresses. UW-Madison faculty, staff and students within the UW HCC may only use e-mail addresses provided by UW-Madison for work purposes (for faculty and staff) and when e-mailing PHI for educational purposes (for students). Use of personal or third-party email addresses to transmit PHI is **strictly prohibited**.

5.2 Use of Automatic Email Forwarding by Rule.

5.2.1 UW-Madison faculty, staff or students in the UW ACE are **strictly prohibited** from using automatic forwarding by rule to direct all e-mail from their UW-Madison email addresses to third-party e-mail accounts outside of the UW ACE.

5.2.2 UW-Madison faculty, staff or students in the UW HCC but not in the UW ACE are **strictly prohibited** from using automatic forwarding by rule to direct all email from their UW-Madison email addresses to third-party email accounts outside of the UW HCC.

5.2.3 UW-Madison may avail itself of security controls available through its approved and licensed technologies to ensure compliance with these auto-forwarding limitations. HIPAA Security Coordinators will collaborate with the HIPAA Privacy and HIPAA Security Officers to develop procedures to enforce these auto-forwarding limitations and will periodically review reports of auto-forwarding throughout the UW HCC to ensure PHI remains within the UW ACE or within the UW HCC as required.

5.2.4 Exceptions to the prohibition on auto-forwarding may only be granted with approval of the HIPAA Privacy and Security Officers.

5.3 UW-Madison faculty, staff or students in the UW HCC who access e-mail remotely or on a mobile device must ensure that other unauthorized individuals do not also have access to the e-mail. They should also enable **device encryption** (which may require adjustments to factory settings on devices) and enroll the device in a Mobile Device Management solution in accordance with procedures developed by their Unit of the UW HCC. Emails containing PHI and accessed remotely should not be printed outside of facilities of the UW HCC. When emails containing PHI are printed (in order to meet the requirements of Section IV, below), they should be printed within facilities of the UW HCC or the UW ACE and then immediately forwarded for scanning and incorporation into the appropriate patient’s medical record.

5.4 Forwarding of provider–patient e-mail communications to a third party (outside of the UW HCC or UW ACE) is prohibited without the written authorization of the patient or the patient’s legally authorized representative.

6. Documentation Requirements

UW-Madison recommends all of the following information be exchanged through patient portals rather than through provider-to-patient emails. However, in the event provider-to-patient email occurs, copies of the following e-mail correspondence must be forwarded to the appropriate Medical Records / Health Information team and placed in the patient’s medical record:

6.1 Notification of test results

6.2 Treatment or follow-up recommendations
6.3 Patient reports about their progress, response to treatment, etc.

6.4 Informed consent process discussions about a treatment or procedure

**Consequences for Non-Compliance**

Failing to comply with this policy may result in discipline for the individual(s) responsible for such non-compliance.

Further, the US Department Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules, and an individual’s non-compliance may result in institutional non-compliance and/or an investigation by OCR. OCR attempts to resolve investigations by obtaining voluntary compliance and entering into Corrective Action Plans and Resolution Agreements. Failures to comply with HIPAA or cooperate with OCR in an investigation may result in civil and/or criminal penalties.

**Supporting Tools**

Additional information may be found at [www.compliance.wisc.edu/hipaa](http://www.compliance.wisc.edu/hipaa)

**Definitions**

1. **External E-mail**: External email is an email message that travels across the public Internet. This type of email, if not encrypted, is not secure nor is it protected in a confidential manner. External e-mail should be considered similar to a “postcard” that might be read by anyone who comes in contact with such a message.

2. **Internal E-mail**: Internal e-mail is an email message that never leaves the confines of the UW network. This type of e-mail uses security software and/or hardware firewalls for protection from intrusion by outsiders. E-mail messages of this type are generally not at risk for being intercepted by outside third parties nor at risk for being viewed by such third parties.

3. **Protected Health Information** (“PHI”): Health information, or healthcare payment information, including demographic information, which identifies the individual or can be used to identify the individual. PHI does not include student records held by educational institutions or employment records held by employers.

4. **University of Wisconsin Affiliated Covered Entity** (“UW ACE”): The UW-Madison Health Care Component (except University Health Services and the State Laboratory of Hygiene), the University of Wisconsin Medical Foundation and the University of Wisconsin Hospital and Clinics. See Privacy Policy # 1.2 “Designation of UW Affiliated Covered Entity”.

5. **UW-Madison Health Care Component** (“UW HCC”): Those units of the University of Wisconsin-Madison that have been designated by the University as part of its health care component under HIPAA. See HIPAA Policy 1.1 “Designation of UW-Madison Health Care Component” for a listing of these units.

**Responsibilities**

HIPAA Privacy Officer
HIPAA Security Officer
**Link to Current Policy**

[TBD]

**Link to Related Policies**

[https://compliance.wisc.edu/policies-and-forms/](https://compliance.wisc.edu/policies-and-forms/)

**Link to Policy History**

N/A

**Review / Approval**

- HIPAA Executive Board, March 26, 2020
- HIPAA Privacy and Security Operations Committee, October 10, 2019