

---

**University of Wisconsin-Madison  
Policy and Procedure**

Policy Number: 8.6  
Policy Title: E-mail Communications Involving Protected Health Information  
Effective Date: March 14, 2004  
Last Revision Date: June 3, 2015  
Page 1 of 6

---

**I. Policy**

The UW-Madison maintains the privacy, confidentiality and security of patients' protected health information. This policy sets forth procedures, limitations and safeguards which must be undertaken when using e-mail to transmit protected health information and to communicate with patients.

UW-Madison protects and safeguards protected health information when communicating with patients via external e-mail. An external e-mail communication that involves protected health information is labeled CONFIDENTIAL, is encrypted wherever possible, and is noted in the patient's medical record. UW-Madison recognizes that encryption is not always easily available to patients, and therefore, UW-Madison faculty and staff, when using unencrypted external e-mail to communicate to patients, must undertake to inform patients about the process and risks of communicating protected health information by e-mail, and must take reasonable measures to safeguard the content and transmission of such external e-mail. Under no circumstances may an HIV test result or treatment record information involving mental health care or alcohol or drug addiction be sent via e-mail.

**II. Definitions**

- A. External E-mail: External email means 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.
- B. Internal E-mail: Internal e-mail is an email-message that never leaves the confines of the UW network. This would include any e-mail message sent to and from an address which includes as its suffix "wisc.edu" or "uwhealth.org". This type of e-mail is protected from intrusion by outside users by security software and /or hardware firewalls. 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.
- C. 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

---

**University of Wisconsin-Madison  
Policy and Procedure**

Policy Number: 8.6  
Policy Title: E-mail Communications Involving Protected Health Information  
Effective Date: March 14, 2004  
Last Revision Date: June 3, 2015  
Page 2 of 6

---

does not include student records held by educational institutions or employment records held by employers.

- D. 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”.
- E. 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 Privacy Policy # 1.1 “Designation of UW-Madison Health Care Component” for a listing of these units.

### **III. Procedures**

- A. Communicating with Patients by E-mail
  - 1. Whenever possible, patients must be encouraged to use MyChart for sending electronic communications to their providers. This ensures that such communications are appropriately documented within the patient’s electronic health record.
  - 2. Before corresponding 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 provide the patient with information substantially in the same form as the attached “Provider – Patient E-mail Information and Consent” and “Guidelines for Using E-mail” explaining the conditions and security risks in using e-mail. If the patient initiates e-mail correspondence prior to an opportunity to discuss e-mail as an option, the health care provider shall e-mail or mail a copy of the information to the patient. Receipt and signed acceptance of the “Provider – Patient E-mail Information and Consent” shall be maintained in the patient’s chart to demonstrate the patient’s agreement to communicate via e-mail.

---

**University of Wisconsin-Madison  
Policy and Procedure**

Policy Number: 8.6  
Policy Title: E-mail Communications Involving Protected Health Information  
Effective Date: March 14, 2004  
Last Revision Date: June 3, 2015  
Page 3 of 6

---

3. Graphs, links, and attachments may be a problem for some patients. Providers should send simple text messages unless it is known that the patient has the software to deal with complex messages.
4. 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. 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, please call your provider's clinic.

B. Communicating PHI by E-mail Inside "wisc.edu"

1. Electronic Storage. UW-Madison faculty, staff and students store e-mail messages containing PHI only on equipment which is within the control and security of UW-Madison or UW Health.
2. UW-Madison E-mail Addresses. UW-Madison faculty, staff and students only use e-mail addresses provided by UW-Madison or UW Health. These e-mail addresses always end in "wisc.edu" or "uwhealth.org". Use of personal or home e-mail addresses to transmit PHI is **strictly prohibited**.
3. E-Mail Client Servers. UW-Madison faculty, staff and students use only UW-Madison or UW Health provided e-mail client servers to read and send e-mail. Use of web e-mail clients, such as Yahoo, Hotmail, and Netscape Mail is prohibited because these e-mail clients use POP to physically copy the e-mail to equipment owned and operated outside of UW-Madison and/or UW Health.
4. Identifiable PHI Limits. Except as allowed for patient-to-physician and physician-to-patient email pursuant to patient

---

**University of Wisconsin-Madison  
Policy and Procedure**

Policy Number: 8.6  
Policy Title: E-mail Communications Involving Protected Health Information  
Effective Date: March 14, 2004  
Last Revision Date: June 3, 2015  
Page 4 of 6

---

consent as outlined above, UW-Madison faculty, staff and students use e-mail to send PHI only if the e-mail is sent within UW-Madison or UW Health. This means the recipient must also be an authorized user of a UW-Madison or UW Health provided “wisc.edu” or “uwhealth.org” e-mail address.

- C. Communicating PHI by E-mail Outside “wisc.edu”. External e-mail sent to addresses outside of “wisc.edu” or “uwhealth.org” travels over the Internet. Therefore, when communicating with clinicians or other health care entity outside of UW Health via e-mail (e.g. referral physicians), PHI may not be included in any portion of the message unless the message is encrypted. Providers needing to communicate with clinicians outside of UW Health via e-mail must consult with their Departmental IT before sending an e-mail for the first time to a specific provider or a specific health care entity to ensure appropriate encryption.
- D. Other Standards for E-mail Communications
1. Criteria for Use. Any health care provider wishing to communicate via e-mail with patients is strongly encouraged to 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 and/or face-to-face communication with the patient. The health care provider should also consider his/her capacity to handle and manage e-mail communication with his/her patients
  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:

---

**University of Wisconsin-Madison  
Policy and Procedure**

Policy Number: 8.6  
Policy Title: E-mail Communications Involving Protected Health Information  
Effective Date: March 14, 2004  
Last Revision Date: June 3, 2015  
Page 5 of 6

---

- a. The reason a response is not forthcoming within the standard time period; and
  - b. When a material response may be expected; or
  - c. Advising the patient on a preferred/alternative method of communication and/or treatment delivery.
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 the correspondent that the health care provider is not available to answer e-mail.

#### General Security

1. Any UW-Madison faculty, staff or students that receive e-mails containing PHI are **strictly prohibited** from using automatic forward to send e-mail to a personal e-mail account.
2. If faculty, staff or students access e-mail from home, they must insure that other members of their household do not have access to the e-mail. No copies of e-mails should be printed except for those described in Section IV below. Any printing must be done within the unit of the HCC and immediately placed in the patient's medical record and/or shredded after scanning.
2. Forwarding of provider – patient e-mail communications to a third party (outside of the UW HCC or UW ACE) is prohibited without the written permission of the patient or the patient's legally authorized representative.

#### **IV. Documentation Requests**

Copies of the following e-mail correspondence shall be placed in the patient's medical record:

- Notification of test results

---

**University of Wisconsin-Madison  
Policy and Procedure**

Policy Number: 8.6  
Policy Title: E-mail Communications Involving Protected Health Information  
Effective Date: March 14, 2004  
Last Revision Date: June 3, 2015  
Page 6 of 6

---

- Treatment or follow-up recommendations
- Patient reports about their progress, response to treatment, etc.
- Informed consent process discussions with the patient about a treatment or procedure.

**V. Forms**

Attached are sample documents that provide e-mail information for patients. These are examples only and are not required or specifically recommended. Please contact the UW-Madison HIPAA Privacy Officer (608-263-9158) for additional information regarding e-mail information for patients.

**VI. References**

45 CFR 164.530(c) (HIPAA Privacy Rule)

**VII. Related Policies**

None.

**VIII. For Further Information**

For further information concerning this policy, please contact the UW-Madison HIPAA Privacy Officer or the appropriate unit HIPAA Privacy Coordinator or sub-Coordinator. Contact information is available within the “Contact Us” tab at [hipaa.wisc.edu](http://hipaa.wisc.edu).

**Reviewed By**

Chancellor  
Chancellor’s Task Force on HIPAA Privacy  
UW-Madison HIPAA Privacy Officer  
UW-Madison Office of Legal Affairs

**Approved By**

Interim HIPAA Privacy and Security Operations Committee