University of Wisconsin-Madison
Policy and Procedures

Policy Number:	8.5
Policy Title:	Security of Faxed, Printed and Copied Documents Containing Protected Health Information
Effective Date:	April 14, 2003
Last Revision Date:	August 21, 2014
Page 1 of 6	

I. Policy

UW-Madison maintains and transmits patient information in a protected and secure manner. Protected health information must be sent in the most secure manner, consistent with the urgency of the information.

This document establishes requirements and guidelines for safeguarding paper documents containing protected health information generated and/or transmitted by facsimile ("fax") machines, printers, and copiers, internal to UW-Madison and at copy pickup/drop-off locations, in compliance with federal and state regulations and statutes.

II. Definitions

A. Business Associate: A person or entity not affiliated with UW-Madison that performs or assists in performing, for or on behalf of any unit in the UW-Madison Health Care Component, business support functions/services that involve the use of Protected Health Information.

B. 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.

C. 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. Faxing PHI

1. Faxing of protected health information should be limited to urgent patient care and treatment purposes whenever possible.

2. Staff members faxing patient information shall take reasonable steps to ensure that the fax transmission is sent to the appropriate destination. When taking a request for information to be faxed, staff should obtain the following information:

   - Name, date of birth of patient, medical record number (if possible)
   - Information requested
   - Reason for request (e.g., continued care)
   - Fax number of requesting party
   - Phone number of requesting party

2. Staff members should always double check the recipient's fax number before pressing the "send" key. When using pre-programmed receiving fax numbers, the numbers should be tested immediately after the first programming to determine accuracy.

3. Whenever possible, documents containing PHI should be accompanied by a separate phone call from the sender, alerting the receiving person of their arrival.

4. A fax cover sheet that includes a confidentiality statement shall be used as a cover page when faxing patient information (see attached sample). The cover sheet shall be filled out completely with the name and department of the sender clearly indicated as well as a description of what was sent.

5. Information and documents that have been faxed "out" shall be gathered immediately after faxing and routed to the appropriate location or destroyed in a confidential manner.

6. Parties receiving faxes from a unit of the UW HCC on a regular or routine basis should be periodically reminded to notify the UW HCC unit if their fax numbers change.

7. If a fax is transmitted in error, contact the person who received the fax to verify destruction of the fax. Report the possible breach as specified in Privacy Policy # 8.8 "Notification and Reporting in the Case of Breach of Unsecured Protected Health Information".

B. Physical Security and Location of Equipment

1. Fax Machines and Printers

a. Fax machines and printers that routinely receive transmissions of protected patient health information shall be placed in secure, non-public areas. Public areas inappropriate for the location of such equipment include, but are not limited to, primary hallways, waiting rooms, multi-use and conference rooms and elevator lobbies.

b. Special consideration should be given to fax machines and printers that receive paper output containing PHI outside of regular business hours (e.g. printers running overnight batch print jobs). This equipment should be located inside a room that is routinely locked outside of regular business hours.

c. Semi-public areas are acceptable locations for printers and fax machines if patients and visitors are accompanied by staff in those locations. Semi-public areas may include, but are not limited to, clinic hallways and work areas where patients are escorted by staff, administrative buildings which have little or no patient traffic, and private office space that is enclosed but not behind locked doors.

2. Copy Machines and Copy Service Pick-Up/Drop-Off Locations

a. Copy machines may be located in areas that are not appropriate for printers and fax machines because a human operator must be present to create output containing PHI on a copy machine, unlike a fax or printer. However, some

copy machines now have both fax and print capabilities. In that case, the copy machine should be located and secured as described in III.B. above. Copy machines should be attended during the copying of PHI.

b. Contracted copy services may be used to copy PHI if the copy originals are secured in transit to and from the copy service location by placing copy originals in a *sealed* container. Sealed containers containing PHI may be left with appropriate employees of the copy service pick-up/drop-off location, and staff shall verify that the copy service will deliver the finished copies to the delivery location in a sealed container.

- Prior to using a contracted for copy service, a Business Associate Agreement must be executed with the copy service and staff must be reasonably certain that the copy service can comply with the terms of the Agreement (See Privacy Policy # 6.1 "Managing Arrangements with Business Associates of the University of Wisconsin-Madison").

C. Procedures for Retrieval of Printed or Faxed Documents

1. Staff should remove output from printers, fax machines and copiers as soon as possible to avoid unauthorized persons from gaining access to the materials.

2. Staff should verify the total number of pages as identified on the fax cover sheet and take care to accurately route the contents.

3. If the fax transmission is illegible, incomplete, or received in error, the sender should be notified immediately. Documents received in error should be immediately destroyed in a confidential manner.

4. Fax transmissions of protected patient health information should be immediately routed to the intended receiver or the patient's record.

D. Use of Courier Services, U.S. Postal Service and Campus Mail to Send PHI

Documents sent in response to routine requests for protected health information should be sent via secure courier, U.S. Post Service or other reliable delivery service.

Campus mail may be used to send PHI only if the envelope/package containing the PHI is sealed as though it is going into the U.S. mail and if the envelope/package is labeled with a warning that the letter/package is confidential and can only be opened by the addressee. Note that most inter-departmental mail envelopes are not appropriate containers because they do not include tamper-evident seals.

IV. Documentation Requirements

None.

V. Forms

Fax Transmission Cover Sheet

VI. References

- 45CFR164.530(c) (HIPAA Privacy Rule)
- § 895.505, Wisconsin Statutes

VII. Related Policies

- Policy Number 3.2 "Uses and Disclosures of Protected Health Information that Require Patient Authorization (Clinical, Non-Research)"
- Policy Number 3.3 "Uses and Disclosures of Protected Health Information Not Requiring Patient Authorization or an Opportunity to Agree or to Object"
- Policy Number 3.9 "Verifying Identity and Authority of Outsiders Seeking Disclosure of a Patient's Protected Health Information"

- Policy Number 6.1 "Managing Arrangements with Business Associates of the University of Wisconsin-Madison"

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.

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