
Department: UW Medicine Information Technology Services

Policy Number: SEC-03.02 Email Standard

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

Purpose

Email provides a convenient and efficient means for communication that supports a wide variety of UW Medicine¹ business needs. However, use of email also entails certain risks and responsibilities, especially when transmitting RESTRICTED or CONFIDENTIAL information. The purpose of this standard is to outline those risks and to define configurations and practices that shall be employed to reduce the risks associated with use of email. This standard also defines ownership for UW Medicine email and describes conditions under which it may be monitored or disclosed.

Definitions

See UW Medicine Information Security policy: *SEC-REF UW Medicine Information Security Program Glossary of Terms*.

Standard

UW Medicine workforce members are required to use University of Washington (u.washington.edu), UW Medicine (uwpn.org, uwp.washington.edu), or affiliates (cumg.washington.edu, seattlecca.org, fhcrc.org, psbc.org, med.va.gov, seattlechildrens.org) email address and services when communicating UW Medicine information.

I. Email Configurations

- A. Login Security: All email clients must use secure protocols during logon to email servers in order to protect the passwords (e.g., IMAP-SSL, POP-SSL, HTTP-SSL, and MAPI with secure RPC.)
- B. Client Server Transmission: UW Medicine email clients must be configured to use secure protocols if CONFIDENTIAL information will be transmitted.
 1. Web-based email clients must use HTTP with SSL (HTTPS) for sending and receiving email.

¹ For the purposes of HIPAA, UW Medicine includes the following entities: University of Washington Medical Center and Clinics; Harborview Medical Center and Clinics; UW Medicine Neighborhood Clinics (University of Washington Physicians Network); UW Physicians Sports Medicine Clinic; Hall Health Primary Care Center; University of Washington Physicians; UW Medicine Eastside Specialty Center, as well as certain services and activities that support UW Medicine that are performed by non-healthcare components of the University of Washington as defined within Privacy Policy PP-01 Use & Disclosure of Protected Health Information – Organizational Requirements. UW School of Medicine is subject to the UW Medicine Information Security Program.

2. Desktop mail clients must use IMAP-SSL or POP-SSL for downloading email from the mailbox server. MAPI systems must use secure RPC.
 3. Desktop mail clients must use SMTP-SSL or MAPI with secure RPC for sending email.
- C. Departmental Servers - Server to Server Transmission: UW Medicine departmental email servers must be configured to support the SMTP STARTTLS command. When using SMTP to transfer email between University of Washington or UW Medicine email servers, the sending system must use STARTTLS to request an encrypted session and the receiving system must honor the STARTTLS request. This will ensure that these email transfers are encrypted via TLS (essentially SSL). If department email servers communicate with other departmental email servers, they also must be configured to encrypt the pathways via TLS. Where technologically feasible, departmental email servers must be required to reject email transfer sessions that are not secure. See Information Security Policy, *SEC-05.03 – Encryption Standard*.
- D. UW Medicine and Affiliates Transmission: UW Medicine Affiliates (Seattle Cancer Care Alliance (SCCA), Children’s Hospital and Regional Medical Center (CHRMC), Children’s University Medical Group (CUMG), and Fred Hutchinson Cancer Research Center (FHCRC)) agree to configure email servers to support the SMTP STARTTLS command. When using SMTP to transfer email between UW Medicine Affiliates and UW Medicine email servers, the sending system must use STARTTLS to request an encrypted session and the receiving system must honor the STARTTLS request. This will ensure that these email transfers are encrypted via TLS (essentially SSL).

II. Email Practices

The most common uses of email are workforce members to workforce members, providers to patients and workforce to non-workforce. These practices must be followed for all email communications:

- Not to place PHI in the subject line.
- Only include the minimum necessary of PHI in the email message.
- Email users, both senders and receivers, are responsible for protection and disposal of information transmitted or stored in email.
- It is the responsibility of the sender to determine whether sending confidential information via email is appropriate.
- Configure an auto reply to acknowledge receipt of the message if circumstances are such that no one will be responding to email for an extended period of time. For assistance:
<http://www.washington.edu/computing/faqs/html/email.autoreply>
- Double-check the addresses of all recipients before sending confidential email.
- Printed email messages must be disposed of properly, based on the data classification.
- UW Medicine workforce members are not permitted to set their University of Washington email accounts to forward automatically to non-University of

Washington email accounts, i.e. personal email accounts such as AOL, Comcast, Hotmail, Yahoo, etc.

- Make sure the following email “signature” or “footer” message is present when communicating PHI:

“The above email may contain patient identifiable or confidential information. Because email is not secure, please be aware of associated risks of email transmission. If you are a patient, communicating to a UW Medicine Provider via email implies your agreement to email communication; see

<http://uwmedicine.washington.edu/Global/Compliance/Pages/Risks-of-Using-Email.aspx>

The information is intended for the individual named above. If you are not the intended recipient, any disclosure, copying, distribution or use of the contents of this information is prohibited. Please notify the sender by reply email, and then destroy all copies of the message and any attachments.

See our Notice of Privacy Practices at

<http://uwmedicine.washington.edu/Global/Compliance/Pages/Notice-Of-Privacy-Practices.aspx>.”

A. Workforce to Workforce Email Communication

Using email for Treatment, Payment, or Healthcare Operations can be done with UW Medicine Workforce Members or to UW Medicine Affiliate Workforce Members (Seattle Cancer Care Alliance (SCCA), Children’s Hospital and Regional Medical Center (CHRM), Children’s University Medical Group (CUMG), Fred Hutchinson Cancer Research Center (FHRC), and Puget Sound Blood Center (PSBC)).

B. Workforce to Patient Email Communication

Email communication between providers and patients provides convenient, direct and efficient communication; the ability to attach educational materials; a good utility for managing simple problems; and improved documentation.

- Providers must include the above email “signature” or “footer” on all patient email communication.
- All email communication that is clinically relevant must be included in the medical record.
- Workforce members may also have the patient complete the “[UW Medicine Agreement for Email Correspondence](#)”.

C. Workforce Member Email to Individuals Outside UW Medicine (Other Than UW Medicine Patients)

Email communication between UW Medicine Workforce members and non-UW Medicine Workforce members that contain electronic Protected Health Information is not allowed, unless appropriate technical safeguards are deployed. Use of email to send PHI outside UW Medicine requires either:

- End-to-end encryption using technologies such as S/MIME and GPG
- Encryption of attachments

UW Medicine strongly discourages workforce members from emailing CONFIDENTIAL information in this fashion.

III. Email Ownership, Monitoring, and Discovery

- A. All email messages and file attachments stored on UW Medicine computers, as well as backup copies stored in any format, are the property of UW Medicine unless otherwise specified by contract. Email messages and attachments sent or received by UW Medicine workforce members and stored on UW Technology systems are also considered property of UW Medicine.

- B. If in the course of normal operation and maintenance of email systems unusual patterns of activity are discovered that suggest a security breach, illegal activity, inappropriate use, or other violations of policy, an investigation by appropriate University of Washington or UW Medicine staff may ensue. The content of email messages may be discovered during this process. Any evidence of illegal or inappropriate behavior will be turned over to the proper authorities.

- C. Under the Public Records Act (RCW 42.17.250 et seq.), if requested by a member of the public, email messages and attachments must be transmitted to the UW Public Records Office for review and possible release. Backup copies of deleted messages and documents are also subject to disclosure via the Public Records Act. Unless protected by legal privilege, electronic messaging is also subject to discovery in litigation. This applies to electronic messaging on disk or on a backup medium. Like other forms of records, and regardless of retention requirements, electronic messaging pertaining to pending audits, or judicial or public disclosure proceedings, must not be destroyed until the audit or legal proceeding is resolved.

References:

- I. 45 CFR Part 164 Section 164.312 (a)(1) Access Control
- II. 45 CFR Part 164 Section 164.312, (e)(1) Transmission Security
- III. American Medical Information Association (AMIA) Guidelines for the Clinical Use of Electronic Mail with Patients, Jan/Feb 1998
- IV. Association of Health Information Management Association (AHIMA) Practice Brief: E-mail Security, February 2000.

UW Medicine IT Services: _____ Date: _____
James S. Fine, M.D., CIO, ISO
