Purpose

The purpose of this policy is to provide all UW Medicine workforce members with specific requirements for safeguarding patient information in all forms (including verbal, paper, and electronic), and in all locations. This policy supports other UW Medicine Compliance policies governing the access, use and disclosure of patient information.

Definitions

- **Patient Information**: Any information (verbal, paper or electronic) created or received by UW Medicine that relates to the past, present, or future physical or mental health or condition of an individual; or relates to the provision of healthcare to an individual; or relates to the past, present, or future payment for the provision of healthcare to an individual; and, either identifies the individual or provides a reasonable basis to believe the information can be used to identify the individual.

Policy

All UW Medicine workforce members and business associates must safeguard patient information at all times (on and off-site). Workforce members are personally and professionally responsible for reasonably and appropriately protecting the privacy, security, and confidentiality of any information to which they are given access.

I. **Patient Information - Verbal**

   Workforce members must:
   - Monitor conversations carefully, taking care to be aware of who is around them and what information could be overheard
   - Hold discussions about patient information in areas where patients, visitors, and workforce members who are not involved in the patient’s care cannot overhear and then speak in a controlled volume.
• Avoid discharging or counseling patients in the hallway, discussing cases in work areas or at the front desk, and making telephone calls to ancillary providers.
• Only discuss patient information in the appropriate workplace setting and only with those who have a need-to-know and the authority to receive the information.
• Strictly limit the amount of patient information discussed to the minimum amount necessary to perform authorized activities or duties.

II. Patient Information - Paper
Workforce members must keep paper-based patient information out of view of patients, visitors, and workforce members who are not involved in the patient’s care.

A) Onsite
• Ensure that patients and visitors are not able to read or reach for paperwork in the work areas where it’s processed.
• Close or flip over charts and files containing patient information when they are not in use.
• Never leave patient information unattended in exam rooms or work areas.
• Dispose of documents containing PHI that are no longer needed in appropriate locked bins.

B) Offsite
Workforce members who must take patient information off site to perform an authorized activity or duty must execute appropriate safeguards. The same requirements for protecting patient information apply when the information is off site.

• Patient information taken off site must be kept fully secured, remain in the workforce member’s physical possession during transit, never left unattended, and never left in any mode of transport (even if the mode of transport is locked).
• Patient information taken off site must be secured at that location, stored in a suitable locked receptacle when not in use or unattended, and removed from printers immediately.
• Disposal of patient information must be done in a secure and confidential manner.

III. Patient Information - Electronic
Workforce members must adhere to UW Medicine Information Security policies: http://security.uwmedicine.org/guidance/policy/default.asp
IV. **Displayed Patient Information**

Workforce members must minimize the use of PHI displayed in patient care areas (e.g., white boards), applying the following rules:

- If names are displayed, use patients’ initials or first initial, last name **UNLESS** using abbreviated name may compromise patient safety.
- Under no circumstance should medical conditions be associated with patient names in public areas.

Workforce members may use patient sign-in sheets or call out patient names in waiting rooms under the following circumstances:

- When reasonable safeguards are in place (patients are not called out by their full names (call for Ms. Smith or Beth).
- When using the minimum amount of patient information necessary. For example, limit information on sign-in sheets to the minimum necessary for the purpose of signing in (i.e., the medical problem for which the patient is being seen is not necessary information for the sign-in process).

V. **Appointment Reminders and Telephone Messages**

Workforce members must minimize the amount of patient information used to leave appointment reminders or telephone messages, applying the following guidelines:

- When a patient is not home and you are directed to voice messaging, provide your name, number, the UW Medicine entity for whom you are calling, and other information which is minimally necessary to confirm an appointment or request a return phone call.
- When a patient is not home and you reach a family member or other person, use professional judgment to determine the minimum necessary information to disclose and ensure that the disclosure is in the best interest of the patient.

**References**

- 45 CFR Parts 164; Section 164.310 (c) Workstation Security, (d) (1) Device and Media Controls
- 45 CFR Part 164; Section 164.310(d)(1) Device and Media Controls; (2) (i) Disposal, (ii) Media Re-use, (iii) Accountability, (iv) Data Backup and Storage
- 45 CFR Part 164; Section 164.530 (c) Standard: Safeguards.
- RCW 18.51.300 Retention and preservation of patient records.
- RCW 40.14 - Preservation and destruction of public records.
- RCW 70.41.190 - Medical records of patients — Retention and preservation.
- UW Records Management Services: http://f2.washington.edu/fm/recmgnt/

Cross References

- SP-03 Workforce Member Policy: http://security.uwmedicine.org/guidance/policy/workforce_member/default.asp

Approvals

__________________________________________  ______________________________
UW Privacy Official  Date
Johnese M. Spisso, Chief Health System Officer, UW Medicine & Vice President for Medical Affairs, UW

Frequently Asked Questions (FAQ)

Q: I have to make a stop at the grocery store on my way home. May I leave patient information locked in my car’s trunk?
A: No. Never leave patient information in any mode of transport (even if it is locked).

Q: I am attending a medical conference. How do I secure patient information?
A: If you are authorized to bring patient information with you to a conference, it must remain in your physical possession or be properly secured – a suitable locked receptacle would be a room safe or hotel safe.
Q: I am working at home. Is leaving patient information locked in my home acceptable security?
A: No. It must remain in your physical possession or be properly secured – a suitable locked receptacle would be a safe or locking cabinet.

Q: May I leave patient information in a locked briefcase?
A: No.

Q: I am working at home. How can I use patient information securely?
A: UW Medicine workforce members can securely access UW Medicine computing resources from a remote location (e.g., home, conference, hotel, etc.) via the Internet by utilizing our Juniper SSL-VPN or Cisco IPSEC-VPN platform. [https://networks.uwmedicine.org/content/secure-remote-access](https://networks.uwmedicine.org/content/secure-remote-access)

**Additional Contacts**

UW Medicine Compliance
206-543-3098
comply@uw.edu

UW Medicine Information Security Program
IT Services Help Desk
206-543-7012
mcsos@u.washington.edu