PURPOSE
The purpose of this policy is to establish the following:
• The process UW Medicine follows to investigate potential breaches of protected health information (PHI);
• UW Medicine’s obligation to notify patients and other parties of a breach of PHI;
• The parties that must be notified and timelines that must be observed;
• Required elements of notifications made to patients; and
• Parties responsible for implementing the policy.

DEFINITIONS
See UW Medicine Compliance Glossary.

POLICY
UW Medicine workforce members shall report potential breaches of patient information. UW Medicine shall review all relevant facts of a reported event to determine if a breach of PHI has occurred, including a formal risk assessment based on required factors to determine the probability that the PHI has been compromised. When a breach is confirmed, UW Medicine shall provide written notification to appropriate parties. The department in which the potential breach occurs shall cooperate with the investigation, assist in remediating identified issues and may be responsible for funding the response and notification of affected patients.

I. Assessment of Potential Breach
UW Medicine reviews all relevant facts of the reported event and determines if the acquisition, access, use or disclosure of PHI:

• Was not for treatment, payment or healthcare operations;
• Was not authorized by the patient;
• Was not otherwise allowed by law; and
• Compromises the security or privacy of the PHI.

If the above facts confirm that an inappropriate action occurred, UW Medicine determines if the inappropriate action meets any of the following exclusion criteria:

• An unintentional acquisition, access or use of PHI by a workforce member or business associate who is acting in good faith within the scope of their authority (providing it does not result in further impermissible use or disclosure);
• An inadvertent disclosure of UW Medicine PHI between two persons who are both authorized to access UW Medicine PHI, providing the information received as a result of such disclosure is not further impermissibly used or disclosed;
• A disclosure of PHI to an unauthorized person, who UW Medicine believes, in good faith, would not reasonably have been able to retain such information; or
• A situation where a formal risk assessment based on required factors demonstrates that there is a low probability that the PHI has been compromised.

If none of the exclusion criteria are met, a breach of PHI is confirmed and UW Medicine completes the notification process.

II. Parties Required to be Notified

• The patient(s).
• The Secretary of the Department of Health and Human Services (DHHS).
• The Washington State Attorney General (must be notified when a privacy breach involves more than 500 Washington state residents).
• The local media (must be notified when a privacy breach involves more than 500 residents of any given state or jurisdiction).

III. Notification Timelines

In general, notifications are made as soon as possible, without unreasonable delay and in no case later than 60 calendar days after the breach discovery date.

Exceptions:

• Notification may be delayed if it would impede a criminal investigation or cause damage to national security.
• If a breach involves less than 500 patients, the timeframe for notification to DHHS is within 60 days of the end of the calendar year in which the breach occurred.

IV. Required Elements of Patient Notifications

A. Written Notifications
1. Must be sent by UW Medicine Compliance and signed by the UW Medicine Chief Privacy Officer or designee.

2. Must be sent by first-class mail to the patient’s last known address (or to the patient’s personal representative if the patient is deceased and UW Medicine has the personal representative’s address). If specified in the patient’s medical record as a preference, the notification may be sent by email.

3. Must contain the following elements:
   • A brief description of what happened, including the breach discovery date and the actual date of the incident, if known;
   • A specific description of the unsecured PHI that was involved in the breach (such as full name, Social Security number, date of birth, home address, account number or disability code);
   • The steps patients should take to protect themselves from potential harm resulting from the breach;
   • A brief description of what UW Medicine is doing to investigate the breach, mitigate losses and help prevent further breaches; and
   • Instructions for obtaining further information, making inquiries and obtaining assistance (including toll-free telephone number, email address, website or postal address).

B. Alternatives to Written Notification

1. If there is insufficient or out-of-date contact information that precludes direct written notification to 10 or more patients, UW Medicine will provide substitute notice. The substitute notices must include a toll-free phone number for obtaining additional information about the breach and may be in one of the following forms:
   • A conspicuous posting for 90 days on the covered entity’s website;
   • A notice in appropriate print or broadcast media that serve geographic areas where affected patients likely reside;
   • An alternative form of written notice, such as by email or by telephone.

2. If imminent misuse of unsecured PHI is suspected, notification may be by telephone or other means.

V. Documentation Requirements
Written documentation must be maintained to demonstrate completion of the following actions:

• Breach risk assessment; and
• Notification to required parties, including copies of letters
VI. Responsibility for Implementation

A. UW Medicine Compliance assesses whether an incident constitutes a breach as defined by the Health Insurance Portability and Accountability Act, makes the relevant recommendation to the UW Medicine Chief Privacy Officer (or designee), makes the required notifications and maintains all documentation.

B. The UW Medicine Chief Privacy Officer (or designee) makes the final breach determination and issues patient notifications.

C. The department in which the breach occurred may be required to pay for the cost of notifying patients.

REGULATORY/LEGISLATION/REFERENCES

- Notification in the Case of Breach of Unsecured Protected Health Information, 45 C.F.R. §164, Subpart D.
- Privacy of Individually Identifiable Health Information, 45 C.F.R. §164, Subpart E.
- RCW 19.86.090 Civil action for damages — Treble damages authorized — Action by governmental entities.
- RCW 42.56.590 Personal information — Notice of security breaches.

PROCEDURE ADDENDUM(s) REFERENCES/LINKS

- UW Medicine Compliance Glossary.
- UW Administrative Policy Statement 2.5 Information Security and Privacy Incident Reporting and Management Policy.

ROLES AND RESPONSIBILITIES

Defined within POLICY.

APPROVALS

Sue Clausen,  
Chief Compliance Officer, UW Medicine
Associate Vice President for Medical Affairs, UW

Date