University Physicians, Inc.

Breach Notification Policy

Original Effective Date: September 1, 2009
Updated: September 3, 2013

PURPOSE: Compliance with final breach notification regulations, effective for breaches discovered on or after September 23, 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act and finalized by the Omnibus Bill, effective March 23, 2013, by requiring HIPAA covered components and their business associates to provide notification following a breach of unsecured protected health information.

POLICY: In the event of a "breach" of unsecured PHI, UPI must notify the patient(s) affected by the breach without unreasonable delay and in no case later than 60 days of discovering the breach.

A breach is considered discovered as of the first day on which the breach is known by UPI or one of its designated business associates. Business associates are required to report any breach to UPI immediately after discovery.

UPI's Privacy Officer will work to timely and accurately report any breach of unsecured PHI according to company policy, HIPAA Omnibus rules, and any and all other Federal and State regulations and interpretive guidelines promulgated there under. The Privacy Officer will maintain all documentation related to the breach for a minimum of six (6) years.

DEFINITIONS:
Breach – Breach means access to PHI or the acquisition, use, or disclosure of PHI in a manner that is not permitted by HIPAA unless a risk assessment demonstrates a low probability that the PHI was compromised.

Protected Health Information – Any oral, written or electronic individually-identifiable health information collected or stored by a facility. Individually-identifiable health information includes demographic information and any information that relates to past, present or future physical or mental condition of an individual.

Unsecured PHI – PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services. PHI that has been encrypted in keeping with UPI Information Security policies is secured.

STAFF RESPONSIBILITIES:

All UPI staff is required to promptly report incidents that raise concerns about the security or privacy of PHI to the UPI Privacy Officer. If the staff person reporting the incident desires anonymity, he/she may use the confidential hotline managed by "EthicsPoint".

PRIVACY OFFICER RESPONSIBILITIES:

The Privacy Officer must promptly document all incident reports that he or she receives, whether the report arrives directly or through a confidential source. If the Privacy Officer determines that an incident clearly does not involve PHI or clearly does not involve improper access to, use of, or disclosure of PHI, he or she shall document that determination and explain to the reporting party why the incident should not have raised concerns. In all other circumstances, the Privacy Officer shall investigate the report his or her conclusion to the reporting party. If the Privacy Officer believes that the incident may constitute a Breach of PHI, as defined by federal law, he or she will conduct a risk assessment in consultation with UPI and SOM General Counsel and, in the case of electronic PHI, with Information Services. If this risk assessment leads to the conclusion that a Breach occurred, the Privacy Officer will document the conclusion and notify the affected patient(s), the Department of Health and Human Services, and, if required by law, the media. If this risk assessment leads to the conclusion that no Breach occurred, the Privacy Officer will document this conclusion.