PRIVACY 2.0 **BREACH NOTIFICATION POLICY**

Scope: All subsidiaries of Universal Health Services, Inc., including facilities and UHS of Delaware Inc. (collectively, "UHS"), including UHS covered entities ("Facilities").

Purpose: To establish procedures for the notification of individuals, prominent media, and the Secretary of the U.S. Department of Health and Human Services, as appropriate, following the discovery of a breach of unsecured protected health information (PHI) by a Facility or its Business Associate(s), and to identify when the unauthorized acquisition, access, use or disclosure of unsecured PHI is a breach for notification purposes.

Definitions:

Terms not defined in this Policy and the UHS HIPAA *Definitions Policy* shall have the meaning as set forth in any related State or Federal privacy law including the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and regulations promulgated there under by the U.S. Department of Health and Human Services ("HHS") at 45 CFR Part 160 and 164, Subparts A and E ("Privacy Regulations" or "Privacy Rule") and Subparts A and C ("Security Regulations" or "Security Rule"), the Health Information Technology for Economic and Clinical Health Act ("HITECH") privacy and security provisions of the American Recovery and Reinvestment Act (Stimulus Act) for Long Term Care, Public Law 111-5, the American Recovery and Reinvestment Act of 2009 ("ARRA"), Title XIII and related regulations.

Breach means an acquisition, access, use, or disclosure of protected health information (PHI) that is not permitted under the Privacy Rule, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. Breach *excludes*: (i) any unintentional acquisition, access, or use of PHI information by a workforce member or person acting under authority of a covered entity or a business associate, if made in good faith and within the scope of authority and does not result in further unauthorized or unlawful use or disclosure; (ii) any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in an unauthorized or unlawful manner; or (iii) a disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Policy:

It is UHS policy to provide notification of the breach of unsecured PHI in accordance with the requirements of HIPAA and The Health Information Technology for Economic and Clinical

Health (HITECH) Act, and implementing regulations. Breach notification is necessary in all situations except where the covered entity or business associate demonstrates that there is a low probability that the protected health information has been compromised, or when one of the exceptions to the definition of a "breach" applies. In addition, documentation sufficient to demonstrate breach notification determinations must be maintained.

Procedure:

Unauthorized Breach of Unsecured PHI

The Facility Privacy Officer will determine whether there has been a breach of unsecured PHI. PHI is "Unsecured" when it is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of encryption and/or destruction. The local Privacy Officer will investigate potential breaches and take steps to mitigate losses and protect against any further breaches. The Facility Privacy Officer will notify the UHS Corporate Compliance Office regarding any potential breaches.

Determining Whether the Disclosure Requires Breach Notification

Not every unauthorized acquisition, access, use or disclosure of unsecured PHI will require notification. To determine whether a breach has occurred, the Facility Privacy Officer will work with the UHS Corporate Compliance Office. First, they will determine whether the incident falls within an exception to the definition of "breach," using the Instructions and Worksheet attached as Exhibits 1 and 2 to this policy.

If the incident *does not fall within one of the exceptions* to the definition of a "breach," then any acquisition, access, use or disclosure of unsecured PHI that is not permitted under the Privacy Rule is presumed to be a breach unless, as described in this Policy, the Facility through its Privacy Officer demonstrates there is a low probability that the PHI has been compromised, based on a risk assessment of at least the following factors, as well as any other relevant factors discovered in the investigation:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
(iii) Whether the protected health in-formation was actually acquired or viewed; and
(iv) The extent to which the risk to the protected health information has been mitigated.

The Facility Privacy Officer, in consultation with senior management at the Facility and the Corporate Compliance Office, will determine this by using the Instructions and Breach Notification Worksheet attached as Exhibit 1 and Exhibit 2 to this Policy. If a determination is made that there is a low probability that the PHI has been compromised, the Facility Privacy

Officer will maintain documentation sufficient to support the determination and to meet the Facility's burden of proof.

Notification to Individuals

The Facility will, following the discovery of a breach of unsecured PHI that requires notification (using the Worksheet), notify each individual whose unsecured PHI has been, or is reasonably believed by the Facility to have been, accessed, acquired, used, or disclosed as a result of such breach.

Timelines for Notification

The Facility Privacy Officer will assure proper breach notification. The Facility Privacy Officer will contact the UHS Corporate Compliance Office in advance of notification, to review the reporting of any breaches.

The Facility will provide the notification required by this Policy as soon as reasonably possible after taking a reasonable time to investigate the circumstances in order to collect and develop the information required to be included in the notice to the individual. Notification will be provided in no case later than 60 calendar days after discovery of a breach.

A breach will be treated as discovered by the Facility as of the first day on which the breach is known or, by exercising reasonable diligence should have been known, by the Facility or any person who is a workforce member, Business Associate, or agent of the Facility (other than the person committing the breach). The time period begins when the incident is first known, not when the investigation is complete, even if it is unclear whether the incident constitutes a breach.

Content of Notification

The notification required by this Policy will be written in plain language, must not include extraneous materials, and must include all of the following:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

4. A brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

5. Contact procedures for individuals to ask questions or learn additional information, which will include a toll-free telephone number, an e-mail address, Web site, or postal address.

Methods of Notification by the Facility

The notification required by this Policy will be provided using the following methods, and may be provided in one or more mailings as information is available:

1. Written Notice:

    a) Written notification will be sent by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by encrypted electronic mail. The notification may be provided in one or more mailings as information is available; or

    b) If the Facility knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification will be sent by first class mail to either the next of kin or personal representative of the individual.

2. Substitute Notice:

    a) Where there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual will be used. Substitute notice need not be provided in the case in which there is insufficient or out-of- date contact information that precludes written notification to the next of kin or personal representative of the individual.

    b) When there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

    c) When there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice will:

        - Be in a form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the Facility, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

- Must include a toll-free number that remains active for at least 90 days where the individual can learn whether the individual's unsecured PHI may have been included in the breach.

3. Additional Notice in Urgent Situations:

In any case the Facility deems to require urgency because of possible imminent misuse of unsecured PHI, the Facility may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided for in this Policy.

4. Notification to the Media

For a breach of unsecured PHI involving 500 or more residents of a State or jurisdiction (city/county), the Facility Privacy Officer will notify prominent media outlets serving the State or jurisdiction. The Facility Privacy Officer will work with the UHS Corporate Compliance Office for notifications involving 500 or more individuals.

Deadline for Media Notification: Except in the case of a law enforcement delay as described below, the Facility will provide the media notification required above without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

Content of Notification: The Notification to the Media will include the same information as is required for the Notification to Individuals.

5. Notification to the Secretary of HHS

The Facility will, following the discovery of a breach of unsecured PHI, notify the Secretary of the U.S. Department of Health and Human Services, as follows:

Breaches Involving 500 or More Individuals: For breaches of unsecured PHI involving 500 or more individuals, the Facility will, except as required for a law enforcement delay as described below, provide notification to the HHS Secretary contemporaneously with the Notification to Individuals, and in the manner prescribed on the HHS Web site. The Facility Privacy Officer will work with the UHS Corporate Compliance Office on breaches involving 500 or more individuals.

Breaches Involving Less Than 500 Individuals: For breaches of unsecured PHI involving less than 500 individuals, the Facility will maintain a log or other documentation of such breaches and, no later than 60 days after the end of each calendar year, provide the notification required for breaches discovered during the preceding calendar year, in the manner prescribed on the HHS Web site. As previously stated, the Facility Privacy

Officer will contact the UHS Corporate Compliance Office to review the reporting of any breaches.

6. Notification to Consumer Reporting Agencies

If 1000 or more individuals are affected and require notification at one time, the Facility must notify, without unreasonable delay, national Consumer Reporting Agencies (that compile or maintain files on consumers on a nationwide basis) of the timing, distribution, and content of the notifications. The Facility Privacy Officer will work with the UHS Corporate Compliance Office on these notifications.

Notification by a Business Associate

A Business Associate will be required, following the discovery of a breach of unsecured PHI, to notify the Facility of such breach in accordance with the procedure set forth in their Business Associate Agreement and as required by law.

Law Enforcement Delay

If a law enforcement official states to the Facility or Business Associate that a notification, notice, or posting required under this policy would impede a criminal investigation or cause damage to national security, the Facility or Business Associate will:

1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

Additional State Law Notification Requirements

State law may impose additional breach notification requirements. If the Facility has any questions regarding its state requirements for breach notification, it will contact the UHS Corporate Compliance Office.

References:

45 C.F.R. Subpart D

Related UHS Policies:

UHS Privacy 16.0 *Disclosures for Law Enforcement Purposes*

UHS Privacy 18.0 *Patient Rights Under the HIPAA Privacy Rule*

UHS Privacy 27.0 *Business Associate Agreements*

Revision Dates:	**10-12-2017; 11-16-2015; 07-22-2013**
Implementation Date:	**07-25-2011**
Reviewed and Approved by:	**UHS Compliance Committee**