TO: Health Sciences IT Managers

FROM: Chris Kidd

DATE: September 16, 2009

RE: Protected Health Information Breach Notification Requirements

The purpose of this letter is to inform you that as of September 23, 2009, The University of Utah (including Health Sciences) will be subject to new data breach notification requirements with regard to protected health information (PHI).

As such, a new University Rule is being implemented that requires reporting of a breach of protected health information to the Health Sciences Help Desk (801-587-6000) as soon possible, but no later than 24 hours after the discovery of the breach. Immediate reporting is necessary to comply with the 60-day time limit for notification of patients and research participants about the breach of their PHI.

A breach is the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of that information. A breach can be avoided by securing information through the use of a technology or methodology (described below) that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals.

- **Encryption.** The use of a National Institutes of Standards and Technology (“NIST”) approved algorithm and procedure is preferred. The use of NIST approved standards will become mandatory over time.
- **Destruction.** Paper, film, or other hard copy must be shredded or destroyed at end-of-life or use such that the PHI cannot be read or otherwise reconstructed and is rendered unusable, unreadable, or indecipherable.
- Electronic media containing PHI must be cleared, purged, or destroyed such that the PHI cannot be retrieved.
- Redaction of paper records is not an approved method of rendering PHI unusable, unreadable, or indecipherable.

Even if you are not subject to HIPAA, you must report any breaches involving PHI. This applies to PHI used in all settings – administrative/operational, clinical, academic, or research.

**Action Items for IT Managers and Staff**

1. Review the examples of data breaches (on page 2).
2. Review data being sent to and from your system(s). Protected health information that is transmitted to, or received from, outside the Health Sciences network must be encrypted.
3. Laptops and tapes containing protected health information must be encrypted. Departments should begin making plans to encrypt or eliminate the use of USB drives.
4. Review your media destruction procedures to ensure it meets the standard identified above.
Examples of Data Breaches
The following is a non-exhaustive list of reportable data breaches:

- Lost or stolen laptops storing PHI.
- Accessing PHI without a business need to know.
- Lost or stolen USB/thumb drives with unencrypted PHI.
- Any unencrypted PHI sent outside of the Health Sciences. This includes using unsecure protocols, such as FTP and Telnet, and not encrypting web pages when patient information is being transmitted.
- Unencrypted e-mails that have been sent outside of the Health Sciences (i.e. without “PHI” in the subject line).
- Faxes sent to the wrong fax machine outside of Health Sciences.
- Paper with PHI not disposed of properly – i.e. shredded.
- CD, DVD, floppies, backup tapes that have not been destroyed at end-of-life.
- Information delivered to the wrong patient using the postal service, courier, or other delivery method.
- Information being sent to the wrong patient or person.

Breaches must be reported to the Health Sciences Help Desk within 24 hours of discovery.

HITECH requirements do not change your obligation to safeguard PHI under the HIPAA Privacy and Security Rules.

Additional information will be provided at the October 7th IT Manager’s meeting. Please feel free to contact me if you have any questions regarding this information. Thank you for all you do to ensure this information is protected.