TEMPLE UNIVERSITY HEALTH SYSTEM
INFORMATION SERVICES & TECHNOLOGY
POLICIES AND PROCEDURES

NUMBER:	0311
TITLE:	Electronic Storage Data Breach Notification Policy
EFFECTIVE DATE:	12-01-2014
LAST REVISED:	12-01-2014
LAST REVIEWED:	12-01-2014
REFERENCES:	TUHS HEALTH INFORMATION – HIPAA Privacy and Security Supplement
ATTACHMENTS:	N/A

PURPOSE

TUHS utilizes electronic Protected Health Information (PHI) to conduct daily business. If any of this information is affected by a breach or accidental loss of data contained on electronic storage, the US federal government has specific requirements for how to notify affected customers, known as the Breach Notification Rule, which is available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.

DEFINITIONS

Electronic Storage – Fixed or removable hard drives contained in computers, servers, or a Storage Area Network (SAN), flash (USB) drives, optical media (CD, DVD, Magneto-Optical), solid-state disk storage, or tape media.

Data Breach – A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual. This includes the loss of any unencrypted data stored on electronic storage.

POLICY

If there is any suspicion of a data breach involving electronic storage within systems under the purview of Information Services & Technology, it is the responsibility of the individual to notify the Chief Information Security Officer.

The Chief Information Security Officer will then ascertain the incident, including the electronic storage involved, and summarize the initial findings.

The Chief Information Security Officer will then notify the Chief Information Officer and Corporate Compliance Officer of the initial findings, and then work under the direction of the Corporate Compliance and Privacy Officer to determine the overall impact and resolve the issue.

The Corporate Compliance and Privacy Officer will evaluate the information gathered during the investigation to determine whether there is objective evidence that there is a low probability that the PHI has been compromised. In the event that the disclosure is determined to be a breach of unsecured PHI, the Corporate Compliance and Privacy Officer will take the following actions.

a. Notify the patient in writing of the nature of the incident, the type of PHI that was compromised, what was done to mitigate the issue and what the patient can do to protect themselves no later than 60 days following the discovery of a breach.

b. Enter the incident in the HIPAA incident report log to be reported to the HHS Secretary at the end of the calendar year, unless the breach involves 500 or more individuals.

c. Breaches of unsecured PHI involving 500 or more individuals require patient, agency and media notifications no later than 60 days following the discovery of a breach.

d. Recommend mitigating measures including disciplinary action and re-education.

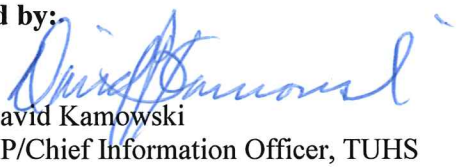
POLICY APPROVAL PAGE

Recommended by:

Mitchell B. Parker
Chief Information Security Officer, TUHS
Date: 12-01-2014

Maribel Valentin, Esquire
Corporate Compliance and Privacy Officer, TUHS
Date: 12-01-2014

Approved by:



David Kamowski
VP/Chief Information Officer, TUHS
Date: 12-01-2014