

TEMPLE UNIVERSITY HEALTH SYSTEM INFORMATION SERVICES AND TECHNOLOGY POLICIES AND PROCEDURES

NUMBER: TUHS-IS-0311
TITLE: Electronic Storage Data Breach Notification Policy
EFFECTIVE DATE: 12-01-2014
LAST REVISED: 05-28-2019
LAST REVIEWED: 05-28-2019
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 HHS/OCR Breach Notification Rule.

DEFINITIONS

Electronic Storage – Fixed or removable hard drives contained in computers, servers, Storage Area Network (SAN), flash (USB) drives, optical media (CD, DVD), solid-state disk 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 PHI 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 IS&T, it is the responsibility of the individual to notify the Chief Information Security Officer (CISO).

The CISO will then ascertain the incident, including the electronic storage involved, and summarize the initial findings.

The CISO will then notify the Chief Information Officer (CIO) and Corporate Compliance Officer (CCO) of the initial findings, and then work under the direction of the CCO to determine the overall impact and resolve the issue.

The CCO 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 CCO will take the following actions:

NOTE:

Refer to the on-line version of this policy for the most current information. Printed copies of this policy may not be current.

Use of this document is limited to Temple University Health System staff only. It is not to be copied or distributed outside of the institution without Administrative permission.


DATE: 05-28-2019

- 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 the breach.
- Enter the incident in the HIPAA incident report log to be reported to HHS/OCR at the end of the calendar year, unless the breach involved 500 or more individuals.
- Breaches of unsecured PHI involving 500 or more individuals require patient, agency and media notifications no later than 60 days following the discovery of the breach.
- Recommend mitigating measures including disciplinary action and re-education.

Compliance to Related Standards and Regulations

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

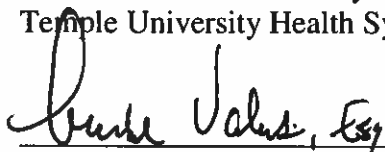
Recommended by:



Stephen Felicetti
Chief Information Security Officer
Temple University Health System



Date Signed



Maribel Valentin, Esquire
Senior Counsel, Corporate Compliance and Privacy Officer
Temple University Health System



Date Signed

Approved by:


David Kamowski
VP / Chief Information Officer
Temple University Health System



Date Signed

NOTE:

Refer to the on-line version of this policy for the most current information. Printed copies of this policy may not be current.

Use of this document is limited to Temple University Health System staff only. It is not to be copied or distributed outside of the institution without Administrative permission.