

TEMPLE UNIVERSITY HEALTH SYSTEM INFORMATION SERVICES AND TECHNOLOGY POLICIES AND PROCEDURES

NUMBER: TUHS-IS-0314
TITLE: Proactive Breach and Vulnerability Monitoring Response
EFFECTIVE DATE: 09-01-2014
LAST REVISED: 05-28-2019
LAST REVIEWED: 05-28-2019
REFERENCES: TUH-IS-0310, Systems Access Management Policy
 TUHS Corporate Compliance Program
ATTACHMENTS: N/A

PURPOSE

To maintain the security of the TUHS environment, Information Security will work with vendors, external monitoring agencies, Biomedical Engineering, Compliance and Risk Management to craft proper mitigations to issues discovered across all TUHS entities.

POLICY

Information Security will work with the following departments and resources to receive information on information systems and computerized biomedical device vulnerabilities:

Vulnerability Type or Target	Resource
Biomedical Device or Specialized Health IT Applications (PACS, etc.)	Emergency Care Research Institute (ECRI) Databases and Alerts
Reported privacy and security breaches	Email distribution membership: REN-ISAC, NH-ISAC, Cyber Health Working Group, Philly Cyber FBI, InfraGard
Vulnerabilities of systems running Microsoft Windows	Microsoft Security Bulletins and Alerts, US Department of Homeland Security Computer Incident Response Team (US-CERT) Security Bulletins, the Security Focus BUGTRAQ vulnerability mailing list (BUGTRAQ), InfraGard Alerts, Full Disclosure security mailing list (https://seclists.org/fulldisclosure/), on premise vulnerability scanning
Breaches affecting 500 or more individuals (per HITECH)	HHS OCR Website (https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)
Vulnerabilities of systems running Linux	BUGTRAQ, Red Hat Network, on premise vulnerability scanning. Full Disclosure security mailing list (https://seclists.org/fulldisclosure/)
Other reported software vulnerabilities	ECRI Databases, ECRI Alerts, BUGTRAQ mailing

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.

	list, US-CERT Security Bulletins, US-CERT Current Activity, InfraGard Alerts, Full Disclosure security mailing list (https://seclists.org/fulldisclosure/)
Vulnerabilities of systems running Oracle	Oracle Security Alerts mailing list, BUGTRAQ mailing list, Full Disclosure security mailing list (https://seclists.org/fulldisclosure/)
Vulnerabilities of systems running another vendor’s software	Vendor reports, BUGTRAQ mailing list, US-CERT Security Bulletins, US-CERT Current Activity, InfraGard Alerts, Full Disclosure security mailing list (https://seclists.org/fulldisclosure/)

Information Security is responsible for:

- Responding to security breaches or vulnerabilities identified at TUHS:
 - Notify affected staff, including but limited to:
 - Director of Clinical Engineering, TUHS
 - IS&T Directors and Managers
 - Director, Risk Management, TUH
 - Director, Risk Management, Jeanes/FCCC Campus
 - Director, IS&T Technical Services
 - Director, IS&T Customer Support
 - Corporate Compliance and Privacy Officer, TUHS
 - Chief Information Officer, TUHS
 - Staff, as needed
 - Develop mitigation plans with the appropriate staff to reduce or eliminate the impact of the vulnerabilities for affected applications.
 - Execute mitigation plans with the involved parties.
 - Verify mitigation of the issue.
 - Communicate risks to the Corporate Compliance and Privacy Officer and Chief Information Officer that cannot be mitigated in accordance with agreed-upon IT policies and procedures.

Compliance to Related Standards and Regulations

- Paragraph 164.308(a)(2) of the HIPAA Security Rule requires organizations to identify a security official responsible for the development and implementation of the policies and procedures required by this subpart for the entity. The CISO of TUHS fulfills the role of the responsible security official.
- Paragraph 164.308(a)(6)(i) of the HIPAA Security Rule requires organizations to implement policies and procedures to address security incidents.
- Paragraph 164.308(a)(6)(ii) of the HIPAA Security Rule requires organizations to identify and respond to suspected or known security incidents, mitigate, to the extent practicable, the harmful effects of security incidents, and document the incidents and their outcomes.

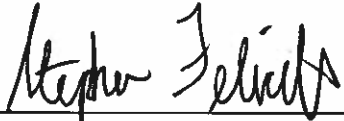
NOTE:

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

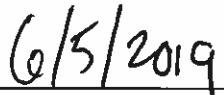
Use of this document is limited to Temple University Health System staff only. It is not to be copied or distributed outside of the institution without Administrative permission.

POLICY APPROVAL PAGE

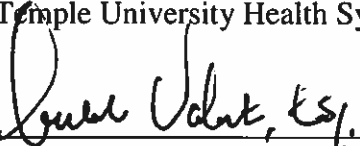
Recommended by:



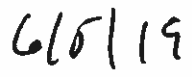
Stephen Felicetti
Chief Information Security Officer
Temple University Health System



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.