ETSU

Policy Title: Security Breach Reporting Procedure (and form)
Policy Manual Section: Computer Security / Transactions
Policy Number: HIP CST 055 B
Effective Date: April 14, 2003
Board Approval Date: November 12, 2014

Review/Revision History:

Reviewed by:	Date:	Revision Number: (i.e. A, B, C)
HIPAA Chair Committee	12/19/02	A
Operations Committee	11/12/2014	B

APPROVED BY:

Signature: _____

Signature: _____

Policy:

It is the policy of ETSU to properly report any security breaches to any network resources. Network resources include but are not limited to servers, main frames, desktops, laptops, tablet PCs, wireless communication devices or any device that has access or remote access to the ETSU network.

Procedure:

1. There are two scenarios for reporting breaches:

    - User suspects a breach on any network device, and
    - Office of Information Technology through intrusion detection and monitoring software.

2. If the user suspects a breach or compromise of any network device the following steps will occur:

    - Complete the security breach report form, and
    - E-mail the form to the system administrator, OIT help desk, and the ETSU network manager.

3. If OIT detects a security breach the following will occur:

   - OIT will complete the security breach report form,
   - e-mail user or system administrator of the PC, server or other network device,
   - OIT will be responsible for determining the problem and the resolution to the security breach,
   - OIT will work with the system administrator or user to resolve the problem and implement any corrective action to prevent future security breaches, and
   - OIT will notify the HIPAA Privacy/Security officer, the chief information officer and the appropriate departmental supervisor of the security breach and any resolutions.

4. The Privacy/Secruity Officer will conduct a risk analysis of the breach to determine the existence of a significant risk to the affected individuals. After September 23, 2013, this risk assessment must include the following:

   - The nature and extend of the protected health information ("PHI") involved, including the types of identifiers and the likelihood of re-identification.
   - The unauthorized person that used the PHI or to whom the disclosure was made.
   - Whether the PHI was actually acquired or viewed.
   - The extent to which the risk to the PHI has been mitigated.

5. If, after investigation, the breach qualifies as a breach under the HITECH Act definition of breach in Subtitle D—Privacy, Part I, § 13400, the data is unsecured, and the breach poses a significant risk to the affected individuals, ETSU must, without unreasonable delay and in no case later than 60 days after the discovery of the breach, notify the individual(s) whose PHI was involved in the breach and notify DHHS.

6. The notice to the individuals must include the following:
   - Description of the types of unsecured PHI that were involved in the breach, such as name, Social Security number, patient number, insurance number, date of birth, home address, disability code, and the like.
   - Brief description of what ETSU is doing to investigate the breach, to mitigate losses, and to protect against further breaches.
   - Contact information for individuals to ask questions or learn additional information, which will include [toll-free telephone number][email address][website url][postal address]. The Privacy Officer shall respond to all such contacts.

7. See Appendix A, below for a sample breach notification letter to be used as a guide in drafting such notices.

8. Unless the contact information is insufficient or out-of-date, the notification shall be by first-class mail to the individual or next-of-kin of the individual or, if specified as a preference by the individual, by email.

9. If the contact information is insufficient or out-of-date, ETSU will use a substitute form of notice, such as, if the breach involves 10 or more individuals for whom information is insufficient or out-of-date, a conspicuous posting on the home page of ETSU's website or a notice in major print or broadcast media in geographic areas in which the individuals affected by the breach likely reside as determined by the Privacy Officer in conjunction with legal and risk management. Such notice will include a toll-free number where the individual can learn whether the individual's unsecured PHI was possibly involved in the breach.

10. If the Security Officer, in consultation with the Privacy Officer determines that the breach requires urgency because of the possible imminent release of unsecured PHI, immediate notification may also be made by telephone or other appropriate means.

11. ETSU will notify the Secretary by visiting the DHHS website and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

12. If the breach involves 500 or more individuals' PHI, ETSU will provide notice to prominent media outlets in the state or jurisdiction of the individuals and immediately to DHHS. The Privacy Officer is responsible for reporting breaches of fewer than 500 individuals to DHHS in the form of a log not later than 60 days from the end of the calendar year. These notifications may be delayed if law enforcement represents that the notification will impede a criminal investigation or damage national security.

13. The Privacy/Security Officer is responsible for processing required notifications under other laws, such as laws requiring reporting of possible identify theft.

14. Under no circumstances may ETSU notify DHHS, the media, or affected individuals without legal review.

Security Breach Report Form

ETSU Office of Information Technology
309 Burgin Dossett, Box 70728
Johnson City, TN 37614

For questions, call the Help Desk at 439-4648 or e-mail: oithelp@etsu.edu

OIT Use Only

Report # _____

Name: _____

Date: _____

I. This section must be completed.

Last Name _____

First Name _____

Phone # _____

Unit/Dept _____

Date of Breach _____

How Breach discovered _____

II. *Check the appropriate box:*

☐ Workstation Tag # _____

☐ Server Server name _____

☐ Other network device (explain)

_____

_____

III. Breach Investigation Details (attach other sheets or documents as required)

IV. Resolution Details (attach other sheets or documents as required)

V. Resolution Acceptance/Close Breach Report

_____ _____
OIT Representative Date

_____ _____
Reporting Party Date

Copies sent to:

☐ HIPAA Officer

☐ OIT Network Manager

Appendix A
Sample Breach Notification Letter

VIA U.S. MAIL, CERTIFIED RETURN RECEIPT REQUESTED
RECEIPT NO. [____ ____ ____ ____ ____]

[Date]

[Name and address of subject of the information that was or may be the subject of a breach]

Dear [name of subject of the breach]:

Here at [name of organization], we understand that personal information is important, and we are committed to protecting information entrusted to our care. This commitment includes notifying individuals if we believe that the security or privacy of their information may have been compromised. We regret to inform you that a recent incident may have exposed your personal information to an unintended audience.

[Enter details of breach or potential breach, such as the following example of an identity theft incident.] On [date], a criminal apparently walked off with one of our employee's laptops while she was going through security at Kansas City International Airport. Her laptop contained clinical records that included, besides the clinical details of your treatment, financial and demographic information that could be used for identity theft. Most likely, the criminal just wanted a laptop that he could pawn, and the data maintained on it was password protected, but we cannot absolutely rule out the possibility of identity theft.

We suggest that you contact any of the three major credit bureaus and have a "fraud alert" placed on your credit file. A fraud alert lets creditors know to contact you before new accounts are opened in your name. You will also be automatically sent copies of your current credit files. You only need to call one of the credit bureaus, for the fraud alert to be placed on all three files. The major credit bureaus and their toll-free telephone numbers are as follows:

- Equifax: (800) 525-6285
- Experian: (888) 397-3742
- TransUnion: (800) 680-7289

[signature]
[Name]
[Title]