HIPAA Security Questions for Researchers

Most important question – does the data set contain Protected Health Information (PHI)?

The University of Toledo defines the data elements which are considered to be PHI in Hospital Policy 3364-100-90-05.

If there is no PHI then the HIPAA regulations do not apply.

When a data set does contain PHI we need to focus on the following areas:

Access to the data

- Are there passwords?
- Who has access to the data?
- Are usernames and passwords shared?
- Who controls creating usernames and passwords?
- How are usernames tracked (who has one, when, etc.)?

Protection of Data

- Where is the data stored?
- Is it password protected?
- Is it encrypted?
- What is the physical security where the data is stored?

Transmission of Data

- Is the data sent anywhere?
- If data is sent off-campus it must be encrypted

E-mail

- E-mail to non-UT addresses is very insecure — 'Almost as secure as a hallway conversation'
- E-mail of PHI should never happen. It is very insecure.

Portable devices

- Even with good username/password controls and encryption, data on portable devices is even more vulnerable than data stored elsewhere With time, any stolen device with PHI can be cracked. Example: An encrypted, password protected zip file can be opened with special password software in just a few minutes (6 character, strong password average elapsed time of 25 minutes).
- With time, any stolen device with PHI can be cracked. Example: An encrypted, password protected zip file can be opened with special password software in just a few minutes (6 character, strong password average elapsed time of 25 minutes).
- There are tools to further secure data portable devices, check with Churton Budd or the Information Security Office for further help.
- Physical protection of portable devices is crucial.

For questions regarding HIPAA compliance, contact:

Mike Lowry
Information Security Officer
419.530.3995

Lynn Hutt
Privacy Officer
419.383.3920