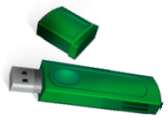
ENCRYPTION TRAINING

JUNE 2013

INFORMATION SECURITY AND PRIVACY OFFICE
THE UNIVERSITY OF UTAH

ATTENTION!

- **ALL** laptops, USB drives and mobile external storage devices that are used to conduct University of Utah Health Sciences business MUST be **whole disk encrypted**. This applies to ALL devices regardless of whether they are personally owned or issued by the UUHSC.



WHAT IS ENCRYPTION?

- Encryption is the translation of data into a “secret code”. It renders the device unreadable to unauthorized users.
- To read an encrypted file, you must have access to a key or password that enables you to decrypt it.
- Encryption is the most effective way to achieve data security.

WHY ARE WE DOING THIS?

- Enforcement of Privacy and Security regulations has greatly increased.
- University of Utah Health Sciences must report the loss or theft of an *unencrypted* laptop, USB or mobile external storage device to the Office of Civil Rights and the Department of Health and Human Services.
- *Unencrypted* devices containing restricted (PHI) data will result in fines and penalties!!!

(HITECH is an extension of HIPAA)

HITECH MONETARY PENALTIES

"Violation Occurred after Reasonable Precautions"

Minimum Penalty	Maximum Penalty
$100	*$1,500,000*

Per Violation...

"Violation Resulted from Reasonable Cause"

Minimum Penalty	Maximum Penalty
$1,000	*$1,500,000*

"Willful Neglect – Corrected Within 30 Days"

Minimum Penalty	Maximum Penalty
$10,000	*$1,500,000*

"Willful Neglect – Uncorrected Violation"

Minimum Penalty	Maximum Penalty
$50,000	*$1,500,000*

University of Utah Health Sciences
Actions in Response to Privacy & Security Violations by Faculty and Staff

Level of Violation	Cause or Motivation	Type of Violation	Examples of Violations	Recommended Actions (One or more)
Level I Errors in handling restricted or sensitive information or in maintaining security measures	• Unintentional • Lack of training • Inexperience • Poor judgment • Poor process	• Clerical Error • Process Error • Technical Error • Judgment Error	• Leaving an active computer screen with access to PHI/PII unattended • Leaving PHI/PII, in any format, unattended in public areas. • Disclosing PHI/PII without identity verification • Discussing PHI/PII in public or other inappropriate areas • Sending PHI/PII to wrong postal, FAX, or e-mail address	• Letter of expectations, including provisions for mitigation, if appropriate • Inclusion of expectations/mitigation steps on performance evaluation • Repeat of Privacy & Security Training • Discussion of policy and procedures • Verbal warning or oral reprimand • New Confidentiality Agreement signed
Level II Breach in the terms of the Confidentiality Agreement and/or University policies concerning use and disclosure of restricted or sensitive information or in maintaining security measures.	• Intentional, but non-malicious • Curiosity • Concern • Compassion • Carelessness • Compulsiveness	• Unauthorized • Non-job related • Stealth	• Failure to properly dispose of paper and electronic media appropriately. • Failure to implement appropriate safeguards for electronic PHI/PII. • Failure to complete required Security and Privacy Training and/or to sign appropriate Confidentiality Agreements • Accessing the record of any person, including co-workers, friends, or family, without a professional need-to-know • Using someone else's computer account • Installing unauthorized software with potential to harm systems • Adding, deleting, or altering electronic information without authorization • Failure to report a security or privacy violation • Failure to establish a Business Associate Agreement • Failure to follow Special Restriction for Out-of-Pocket Payment for Services • Repeated Level I violations	• Final written warning, requiring written corrective action plan in response; ineligible for transfer or promotion for up to 12 months • For faculty, referral to Vice President for review of violation of academic code; • Suspension of information system user privileges • Suspension of employment • Suspension of research projects • Inability to participate in Research for up to 12 months.
Level III Breach in the terms of the Confidentiality Agreement and/or University Policies concerning use and disclosure of restricted or sensitive information, for personal gain or to affect harm on another person	• Malicious intent • Financial gain • Revenge • Protest • Gross Negligence	• Theft, including identity theft • Malicious actions: i.e., alteration or deletion of data; making systems inaccessible	• Access and unauthorized disclosure of PHI/PII for personal gain or to affect harm on another person • Unauthorized access of celebrity or VIP PHI/PII for any reason • Malicious alteration, deletion or removal of PHI/PII, from University facilities • Unauthorized publication or broadcasting of PHI/PII • A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline • Repeated Level I or II Violations	• Suspension of employment; • Suspension of Research Projects; • Termination of information system user privileges; • Referral to VP as violation of faculty code; • Revocation of Medical Staff privileges; • Termination of employment; ineligible for rehire and future information systems access.

University of Utah Health Sciences
Actions in Response to Privacy & Security Violations by Students

Level of Violation	Cause or Motivation	Type of Violation	Examples of Violations	Recommended Actions (One or more)
Level I Errors in handling restricted or sensitive information or in maintaining security measures	• Unintentional • Lack of training • Inexperience • Poor judgment • Poor process	• Clerical Error • Process Error • Technical Error • Judgment Error	• Leaving an active computer screen with access to PHI/PII unattended • Leaving PHI/PII, in any format, unattended in public areas. • Disclosing PHI/PII without identity verification • Discussing PHI/PII in public or other inappropriate areas • DMCA violations • Sending PHI/PII to wrong postal, FAX, or e-mail address	• Letter of expectations, including provisions for mitigation, if appropriate; • Retraining and reevaluation; • Specialized training and evaluation; • Discussion of policy and procedures; • New Confidentiality Agreement signed; • Community Service, as appropriate;
Level II Breach in the terms of the Confidentiality Agreement and/or University policies concerning use and disclosure of restricted or sensitive information or in maintaining security measures.	• Intentional, but non-malicious • Curiosity • Concern • Compassion • Carelessness • Compulsiveness	• Unauthorized • Non-job related • Stealth	• Placing non-shredded documents in inappropriate waste receptacles; • Failure to complete required Security and Privacy Training and/or to sign appropriate Confidentiality Agreements; • Accessing the record of any person, including co-workers, friends, or family, without an authorized need-to-know; • Using someone else's computer account; • Installing unauthorized software with potential to harm systems; • Adding, deleting, or altering electronic information without authorization; • Failure to report a security or privacy violation; • Repeated Level I violations;	• Letter of reprimand, requiring written corrective action plan & acknowledgement of consequences of subsequent infractions; i.e., expulsion, and obligation to make restitution, as appropriate; • Temporary loss of University privileges, including use of University library, parking, computers, and athletic/entertainment functions; • Conduct suspension; • Contract of restitution
Level III Breach in the terms of the Confidentiality Agreement and/or University Policies concerning use and disclosure of restricted or sensitive information, for personal gain or to affect harm on another person	• Malicious intent • Financial gain • Revenge • Protest • Gross Negligence	• Theft, including identity theft • Malicious actions: i.e., alteration or deletion of data; making systems inaccessible	• Access and unauthorized disclosure of PHI/PII for personal gain or to affect harm on another person; • Unauthorized access of celebrity or VIP PHI/PII for any reason; • Malicious alteration, deletion or removal of PHI/PII, from University facilities; • Unauthorized publication or broadcasting of PHI/PII; • A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline; • Repeated Level I or II Violations.	• Expulsion without opportunity to continue at the University of Utah in any status, and ineligible for University privileges, including use of University library, parking, and entertainment/athletic functions; • Contract of Restitution.

MORE REASONS TO ENCRYPT!

- Encryption is the most effective way to achieve data security and privacy.
- **Encryption makes data accessible only by authorized personnel.**
- Encryption is cost effective and a reasonable way to protect our data.
- Encryption supports our commitment of trust.

WHO NEEDS TO ENCRYPT?

This encryption requirement applies to:

All University of Utah Health Sciences Center Departments and Units

WHAT DO I NEED TO DO?

- Encrypt your laptops and mobile external storage devices that are used for UUHSC business purposes, regardless of whether or not they are UUHSC owned or personally owned by *September 30th, 2013*.
- If they are not encrypted after September 30th, 2013, you will be denied access to the network.

ENCRYPTION PROCESS

- Hospitals and Clinics Staff:
  - Contact the Help Desk at **801-587-6000.**
- Everyone Else:
  - Contact your IT manager with questions.

Examples of Acceptable Encryption Software:

PC: PGP, bit locker, TrueCrypt

Mac: PGP, File Vault 2 (OS X 10.7 Lion and above)

ATTESTATION

I have read and understand the new UUHSC Encryption Procedure and understand what is required of me.

- A) I have completed the encryption process and I will only use encrypted laptops, encrypted USB drives and encrypted mobile external storage devices at UUHSC.
- B) I will contact the Hospital Help Desk or my IT Manager, and I will encrypt all laptops, USB drives and mobile external devices I use at UUHSC **before September 30, 2013**. When complete, I will return to this training module and select choice A to verify the encryption process is done.

Submit

Question 1 of 1

CONGRATULATIONS!

You have completed this training module.

ENCRYPTION TRAINING

Contact the Privacy Office at
801-587-9241 with Questions

INFORMATION SECURITY AND PRIVACY OFFICE
THE UNIVERSITY OF UTAH