HIPAA Privacy & Breach Notification Training for ARDC Staff

Barbara M. Holthaus
privacyofficer@utsystem.edu
Office of General Counsel
University of Texas System

August 10, 2015

Webinar Essentials

- Session is currently being recorded, and will be available on the Systemwide Compliance Academy website at http://www.utsystem.edu/offices/systemwide-compliance/systemwide-compliance-academy

WHY ARE WE HERE?

- HIPAA requires all members of the Workforce of a Covered Entity or Business Associate to have initial (and periodic follow up training) on its Privacy & Breach Notification Policies
- Failure to provide and maintain documentation of training is a HIPAA violation and can result in penalties for System Administration
- System Administration is required to sanction employees who violate HIPAA

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996 and HITECH Act

- Privacy , Security, Enforcement and Breach Notification Standards 45 CFR Part 160 & 164

  http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html

- Revisions (Omnibus Rule):

  http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

System Administration's HIPAA Policies

- System Administration's Privacy Policy is INT 166 (it link to the HIPAA PRIVACY MANUAL on the Office of Employee Benefits web page)
- System's Security Policies are UTS 165 and INT 124 (Includes the Acceptable Use Policy
- System Administration's Breach Notification Policy, INT 165, is also on the Policy Library Page. It addresses Texas State Privacy Law, as well as HIPAA, breach requirements

Systemwide Policy Library- UT SYSTEM WEB PAGE

http://www.utsystem.edu/board-of-regents/policy-library

Privacy vs Security

- Privacy- Governs who can and should (authorized individuals) have access to personal information
- Security- Mechanisms for ensuring that only authorized individuals have access to information that is Private

HIPAA Individual* Rights

- Receive a Notice of Privacy Practices- (from the Covered Entity only- not a Business Associate)
- Access your own records (Designated Record Set only-more later)
- Receive an Accounting of Who Has accessed your PHI
- Ask to amend your own records-(Designated Record Set only)
- Ask for restrictions on Disclosures and Use
- Ask for Confidential Communications
- File a Compliant
- Receive a Breach Notification

*patient or health insurance plan member or personal representative of either

HIPAA IN A NUTSHELL

- Federal law that gives individuals rights over their personal health information
- Only Covered Entities and their Business Associate must comply with HIPAA
- Only applies to certain kind of information- Protected Health Information (PHI)
- Requires that PHI be maintained confidentially and securely
- Requires notifications if breach of PHI occurs
- Provides for enforcement and penalties if violated

Basic Rule of HIPAA

Employees **may not** access or disclose PHI **unless**:

- The subject has given written permission
- It is within the scope of an employee's defined job duties; or
- Required or permitted by a specific HIPPA exception

PERSONAL HEALTH INFORMATION (PHI)

PHI is any information that can be used to identify an individual – whether living or deceased – that relates to the individual's past, present, or future physical or mental health or condition, including healthcare services provided and payment for those services.

No Really, What is PHI?

- Realistically, for today's training, it means any data that comes from:
- a medical record
- a health plan
- or a third party that access data from a HIPAA Covered Entity
- IF THAT DATA CONTAINS ANY IDENTIFIERS ABOUT THE INDIVIDUAL TO WHOM IT PERTAINS

Identifiers that make PHI "PHI"

- **Names;**
- **Postal address information (but not including town or city, state, and zip code);**
- **Telephone numbers;**
- **Fax numbers;**
- **Electronic mail addresses;**
- **Social Security numbers;**
- **Medical record numbers;**
- **Health plan beneficiary numbers;**
- **Account numbers;**
- **Certificate/license numbers;**
- **Vehicle identifiers and serial numbers, including license plate numbers;**
- **Device identifiers and serial numbers;**
- **Web Universal Resource Locators (URLs);**
- **Internet Protocol (IP) address numbers;**
- **Biometric identifiers, including finger and voice prints (DNA!!!!) ; and**
- **Full face photographic images and any comparable images.**

What is Not PHI

- Aggregated and de-identified information is not PHI.
- However, even information stripped of an identifier can still be PHI. For example info about a health insurance claim that gives sex, age and a diagnosis could be enough to allow a colleague to identify the individual.

Other Important Exceptions to PHI Definition (not PHI)

- Information Maintained As Employee Records Is Not PHI
- FMLA and sick leave records
- ADA Information

  (however, such info is still subject to other federal and state privacy laws.)

- Education Records & Student Treatment Records Maintained by a Student Health Centers ARE NOT PHI. (That is why most academic institutions are not subject to HIPAA.)

Rule of Thumb

Treat all System data that relates to individual as if it is PHI

- Depends on the context
- Normally you can't tell what category data falls under by looking at it
- Let the Privacy Officer worry about making the final call!

Who Must Comply with HIPAA

- Covered Entities- health care providers that bill insurers, health plans and clearinghouses
- Business Associates ("BA"s)–third parties (often vendors) who perform business functions for a Covered Entity that require access to the Covered Entity's PHI. Can include other governmental entities, too (ex- Attorney General's Office)

System Administration Offices Subject to HIPAA

Covered Entity:

- Office of Employee Benefits (Operates the System's Employee Health Care Plan)

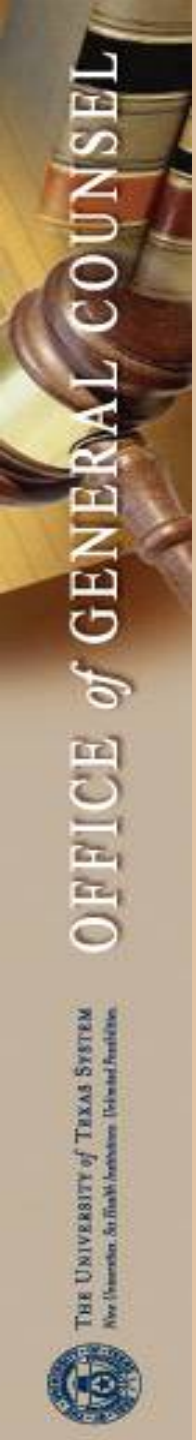
Business Associates:

- Office of General Counsel
- Systemwide Compliance- Including Systemwide and System Admin INFOSEC
- Internal Audit Office
- OTIS
- Systemwide Information Services including;
- OFFICE OF SHARED SERVICES- SERVICES TO SYSTEM INSTITUTIONS THAT ARE COVERED ENTITIES
- (PLUS anyone in ARDC that is accessing Protected Health Information maintained at the ARDC, even if they work for UT Arlington)

The System's Other HIPAA Covered Entities

Not one big happy family. System is not one single Covered Entity. PHI cannot be shared among institutions (or the BOR) without patient consent *unless a specific HIPAA exception applies*

- **UTMB**
- **UT HSC SOUTHWESTERN**
- **UT HSC HOUSTON**
- **UT HSC SAN ANTONIO**
- **UT HSC Tyler**
- **MDACC**
- **UT Austin- Hybrid**
- **UT Dallas- Hybrid**
- **UT Arlington- used to be a Hybrid Entity, Still maintains some medical records subject to HIPAA. Also has a data center that is a Business Associate to other System Covered Entities**
- **UTRGV will be a Covered or Hybrid Entity if it operates a hospital or its physicians begin providing care at another teaching hospital.**



YOU GUYS ARE HIPAA BUSINESS ASSOCIATES

Business Associates

Are directly liable for failure to comply with HIPAA
A Business Associate must :

- Enter into a HIPAA compliant Business Associate Agreement (BAA) with the covered entity, or MOU if between institutions, or if the Business Associate is part of the same legal entity as the Covered Entity, have HIPAA compliant policies
- Use appropriate safeguards to prevent the access, use, or disclosure of PHI other than as permitted by the contract, or BAA, with the covered entity

Business Associates (con't)

- Obtain satisfactory assurances from a subcontractor that appropriate safeguards are in place to prevent the access, use, or disclosure of PHI entrusted to it
- Notify the covered entity upon discovery of any breach of unsecured PHI for which the Business Associate was responsible
- Ensure that its employees and/or those of its subcontractors receive HIPAA training
- Protect PHI to the same degree as a covered entity

Business Associates Using and Disclosing PHI

- BAs are limited to Using and Disclosing PHI only as set forth in the BA Agreement/MOU/routine duties
- Any Use or Disclosure *not* part of the BA's routine duties must be documented must be documented by the BA (report to Privacy Officer)
- Accounting Rule- if requested, BA must produce a list of non-routine disclosures
- Examples: Subpoenas, law enforcement exception, unauthorized acquisition (a breach is a disclosure)
- **All non-routine Disclosures must go through the Privacy Officer/OGC**

Minimum Necessary Rule

- Access within the Covered Entity (or Health Care Component) to PHI must generally be limited to information required to perform a specific, official duties
- Applies to any PHI a Business Associate accesses
- Exception for Payment & Treatment (doesn't apply to Business Associates)

OGCs Business Associate Role

- General Law- accesses PHI for Tort Claim, Employment and other types of litigation. We also access it to provide legal advice to institutions that require access to PHI, such as a HIPAA violation, and to OEB for legal advice regarding the self-funded health plans. We may also provide advice to System Institution offices that are Business Associates that requires access to PHI. Can be Payment, Treatment or other.
- Health Law- accesses PHI to provide its physicians and other employees with litigation assistance involving Med Mal cases- primarily "Treatment" PHI
- Claims accesses PHI to assist in collecting money owed for health services- primarily "Payment" PHI
- Unlikely that the Business Law or Real Estate Sections will ever access PHI.

Other System Administration BA Office's roles

- OTIS and Shared Services- access PHI in computers and servers to retrieve PHI for litigation holds, investigations, technical services, monitor acceptable use, other tech related services
- Audit- if required as part of an audit of a Covered Entity and only access is necessary to the specific audit
- Compliance/Info Sec- as needed to investigate a complaint or breach or security incident

Outsourcing

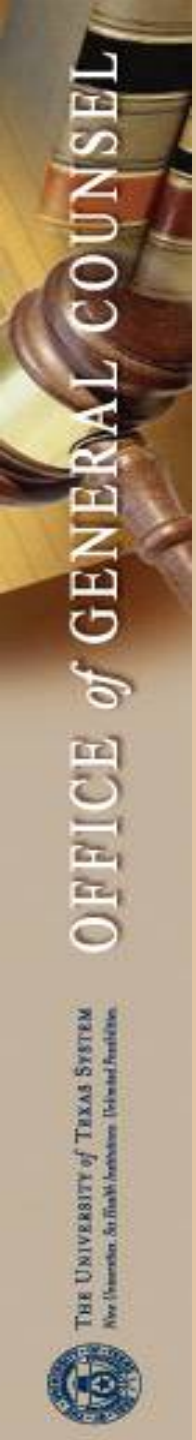
- Offices that outsource data use or creation or store data offsite must have a HIPAA compliant Business Associate Agreement with any vendor or other third party that will use or disclose System PHI
- Applies even if the third party is just storing it- beware of the Cloud!

Safeguarding PHI

- Read and follow the Acceptable Use Policy
- Keep paper documents under lock and key if unattended, dispose of securely, don't take it home- you can't encrypt it. Use an encrypted System laptop or an encrypted thumb drive
- Don't use Drop Box, other cloud based solutions not authorized by Info sec
- Computers, Laptops, Data Bases: Password Protect, encrypt, use encrypted lap top and VPN for telecommuting
- E-mail: Only if Encrypted

Safeguarding PHI (con't)

- Do not create or store PHI on a personal computer or PDA, smart phone
- Oral: Limit use of names, speak softly
- Mailing: Sealed envelope, marked "Confidential"
- FAXing: Mark confidential, verify numbers
- No Social Media (use your head!)



BREACHES

HIPAA AND TEXAS STATE LAW BOTH HAVE BREACH PROVISIONS

Breaches

A breach occurs when information that, by law, must be protected is:

- Lost, stolen, or improperly disposed of (i.e. paper or device upon which the information is recorded cannot be accounted for)
- "Hacked" into by people or mechanized programs that are not authorized to have access
- Accessed by employees for an unauthorized reason (curiosity, identity theft, an email or letter sent to the wrong recipient)

Incident- anything that could be a breach

BREACHES- HIPAA

- Any unauthorized access of PHI- includes access by unauthorized staff (requires harm analysis) that is not encrypted per NIST standards
- Electronic and Paper Data
- System Administration Has a Data Breach Rule- INT 166

BREACHES- HIPAA

- Notify affected individuals within 60 days of when Covered Entity know or should have known of breach
- Law enforcement exception may permit delay but need to document
- Responsible for breaches affecting Business Associates
- Notify DHS within 60 days of breaches affecting 500 or more individuals, by end of calendar year of breached affecting < 500
- Notify media if cannot locate affected individuals

BREACHES- State Law

Texas State Gov't Code §2054.1125 & Tx Business & Com Code 521

- Applies to "Sensitive Data"
- Applies to breaches affecting data in or from an electronic data base
- Applies only if info in unencrypted or person also accesses encryption key
- Exemption for good faith acquisition by employee or agent

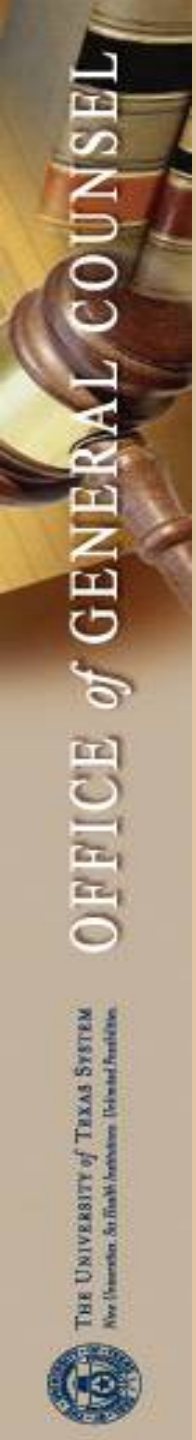
Sensitive Data

Different from PHI. Includes

- Any health or health billing records that are not PHI
  - Include employer/HR records!
  - Includes research data!
- Person's Name plus:
  - SSN
  - Account numbers (Bank, Credit, or Debit plus PIN)
  - Driver's License or government issued ID numbers

System Administration' s Breach Notification Rule INT 165

- Covers HIPAA & State Law Breaches
- MUST notify Privacy Officer & Chief Information Security Officer at UT System *immediately of anything that could be a breach*- don't investigate, just report it
- Breach Response Team appointed by Chancellor will ensure that System investigates, mitigates, and provides all required notices.



ENFORCEMENT and PENALTIES

Reporting Violations and Sanctions

- HIPAA requires Covered Entities and Business Associates to receive and investigate complaints of violations and sanction employees who violate HIPAA any policy
- Employee cannot be sanctioned for reporting a violation
- DHS has authority to investigate and sanction CE's and BA's for non-compliance

Monetary Penalties for HIPAA Violations

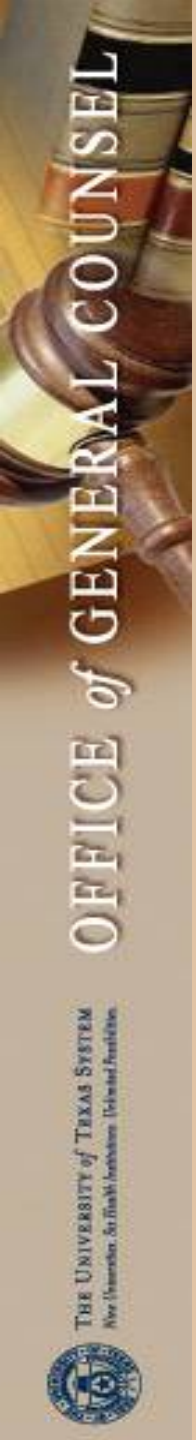
- Covered entity or business associate did not know (and by exercising reasonable diligence would not have known) the act was a HIPAA violation.-$100-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
- HIPAA violation had a reasonable cause and was not due to willful neglect.$1,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
- HIPAA violation was due to willful neglect but the violation was corrected within the required time period.$10,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
- HIPAA violation was due to willful neglect and was not corrected. $50,000 or more for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year

RECAP
HIPAA Business Associates' Responsibilities

- Be Aware of and comply with HIPAA Privacy (and Security) Policies
- Receive HIPAA training on the policies
- Use and Disclose PHI only to perform specific job duties
- Report and ensure documentation of Disclosures if required
- Protect Security of PHI
- Report anything that could constitute a Breach to Security
- Report HIPAA violations to Privacy Officer
- Mitigate harm caused by lack of compliance

RULE OF THUMB

- Treat all data like it is PHI
- Make sure any third party that will work on a system or computer containing PHI has a HIPAA BAA with System Adminsistration
- Report any unauthorized access, even your own
- If some asks you to access data- unless it is a formal part of your job to provide access- ask the Privacy Officer



All righty then!

QUESTIONS???

HIPAA SECURITY

SECURITY RULE PRIMER

THE UNIVERSITY OF TEXAS SYSTEM

AUGUST 2015

TRAINING OBJECTIVES

By the end of this training, you will have knowledge of:

- the HIPAA Security Rule and
- security standards for the protection of electronic protected health information

PRIVACY RULE VS. SECURITY RULE

Privacy Rule

Addresses who may access protected health information (PHI) and under what circumstances. Applies to all forms of PHI, whether electronic, written, or oral.

Security Rule

Complements the Privacy Rule. Addresses **standards** for ensuring access to ePHI by appropriate parties. **Applies to electronic information only**.

HIPAA SECURITY RULE

- Establishes national standards to protect **electronic health information (ePHI)**
- Requires appropriate **administrative, physical**, and **technical safeguards** to ensure the confidentiality, integrity, and security of ePHI

SAFEGUARDS

Required vs. **Addressable** standards

- **Required:** specifications **must be met** by an organization
- **Addressable:** organizations must assess whether safeguard is reasonable and appropriate, given their environment.

If implementing the safeguard is not reasonable and appropriate, **organizations** must document the rationale and **implement an equivalent measure** that would accomplish the same purpose.

ADMINISTRATIVE SAFEGUARDS

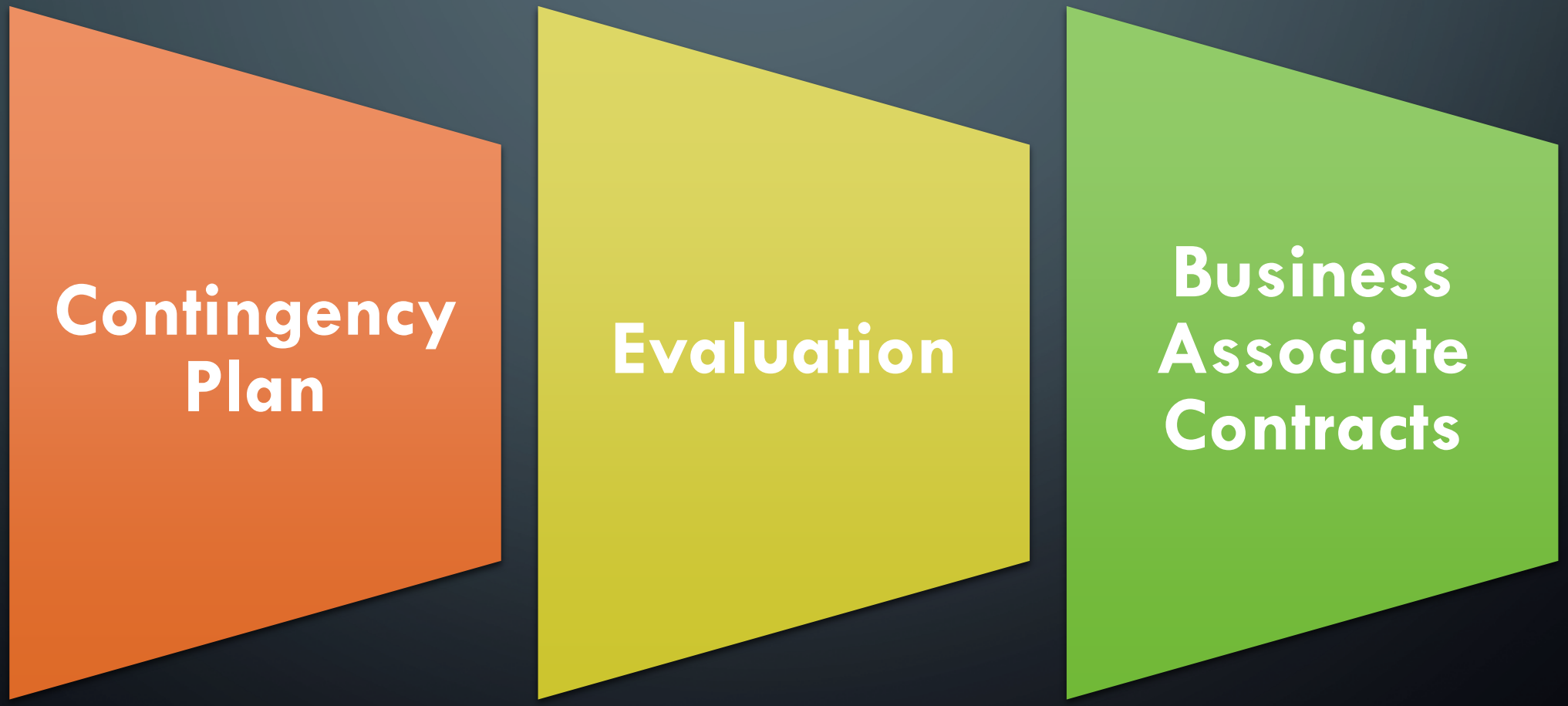
Security Management

Assigned Security Responsibility

Workforce Security

ADMINISTRATIVE SAFEGUARDS

ADMINISTRATIVE SAFEGUARDS



PHYSICAL SAFEGUARDS

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device & Media Controls

TECHNICAL SAFEGUARDS

- Access Controls
- Audit Controls
- Integrity
- Authentication
- Transmission Security

UT SYSTEM POLICIES

The University of Texas System has policies in place to address privacy and security of sensitive and protected health information:

- **UTS165:** Information Resources Use & Security Policy
- **INT124:** Information Resources Acceptable Use & Security Policy
- **INT165:** Breach Notification Policy
- **INT166:** System Administration HIPAA Privacy Policy Manual

QUESTIONS

- **UT System Privacy Officer**
  Barbara Holthaus (bholthaus@utsystem.edu)
- **Common Use Infrastructure Information Security Officer**
  Bill Taylor (btaylor@utsystem.edu)
- **UT System Training Coordinator**
  Becki Mendivil (bmendivil@utsystem.edu)