



THE UNIVERSITY *of* TEXAS SYSTEM  
*Nine Universities. Six Health Institutions. Unlimited Possibilities.*

# The Data Owner's Role in Information Security

THE UNIVERSITY OF TEXAS SYSTEMWIDE COMPLIANCE OFFICE



SYSTEMWIDE COMPLIANCE ACADEMY

PROVIDING COMPLIANCE LEADERSHIP AND GUIDANCE TO THE UNIVERSITY OF TEXAS SYSTEM

**Lewis Watkins, CISO**  
[lwatkins@utsystem.edu](mailto:lwatkins@utsystem.edu)



# The Data Owner's Role



1. Understand the changing information security and regulatory environment.
2. Become familiar with security roles.
3. Answer the question: Who is a "Data Owner"?
4. Understand Data Owner responsibilities.
5. Know the people and tools that can assist Data Owners.



THE UNIVERSITY of TEXAS SYSTEM  
*Nine Universities. Six Health Institutions. Unlimited Possibilities.*

# A Resource for Data Owners



THE UNIVERSITY of TEXAS SYSTEM  
*Nine Universities. Six Health Institutions. Unlimited Possibilities.*

## Information Owner's Guide to Data Protection

- Lessons Learned and Best Practices -

July, 2010

Written at the direction of UT System Chancellor Cigarroa.

### Contents:

- The Threat Landscape
- Learned Lessons & Best Practices
- Security Roles
- What Data Owners need to Know
- What Data Owners need to Do
- Tools
  - Things to Know Checklist
  - Ten Step Owner's Data Protection Plan
  - Best Practices Matrix and Checklist

Download at: [www.utsystem.edu/ciso](http://www.utsystem.edu/ciso)



# Some Lessons Learned

## U. S. Secret Service / Verizon 2010 Breach Report Facts

- 85% of attacks were not complex.
- 96% of breaches were avoidable using simple controls.



## Common Characteristics of UT System incidents

- Most occur within decentralized areas.
- Often the exposed data should long ago have been deleted.
- Often the data involved is not known to exist by anyone.
- Sometimes the data resides on a computer that the Security Office does not know exists.



THE UNIVERSITY of TEXAS SYSTEM  
*Nine Universities. Six Health Institutions. Unlimited Possibilities.*

# The Changing Climate

An aerial photograph of a city skyline at sunset, with a warm orange and yellow glow over the buildings. The word "CHANGE" is overlaid in large, white, sans-serif capital letters in the center of the image.

CHANGE



“Oh Toto, I don’t think we are in Kansas anymore!”

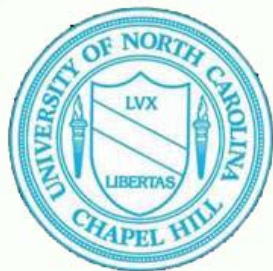
- State of Virginia medical data held for ransom (**outsider**)
- San Francisco network held hostage (**insider**)
- Slacker harms Univ. of Utah by PHI exposure (**partner**)
- Stuxnet – targets Iran nuclear program (**nation-state**)
- Targeted, Advanced Persistent Threats (APT) (**nation-states and organized crime**)
- UNC Professor fighting HIPAA related firing (**outsider**)
- Drive-by malware – mostly unseen (**nation-states and organized crime**)
- Bots, Bots, Bots – (spam, malware dist.) (**organized crime**)

**Once an idea goes public, others quickly imitate!**



THE UNIVERSITY of TEXAS SYSTEM  
*Nine Universities. Six Health Institutions. Unlimited Possibilities.*

## The Stakes are High



### University of North Carolina Researcher Disciplined

**Professor Yankaskas, an epidemiologist, supervised a project for 15 years that compiles and analyzes mammogram data.**

**A hacker infiltrated a database she oversees. The breach endangered 180,000 patient files, including about 114,000 Social Security numbers.**

**Yankaskas says she shouldn't be held responsible for a lapse by an information technology staffer. But UNC disagreed. She's been demoted from full to associate professor and her pay cut from \$178,000 a year to \$93,000.**



THE UNIVERSITY of TEXAS SYSTEM  
*Nine Universities. Six Health Institutions. Unlimited Possibilities.*

... and they are Rising!



## HHS Flexes HIPAA Enforcement Muscles

This week, the U.S. Department of Health and Human Services sent warnings that it is serious about enforcement now that it can finally do something to discourage violations. HHS imposed a **\$4.3 million** civil penalty on Cignet Health for violating HIPAA privacy provisions and settled for **\$1 million** with Massachusetts General Hospital for HIPAA privacy violations.

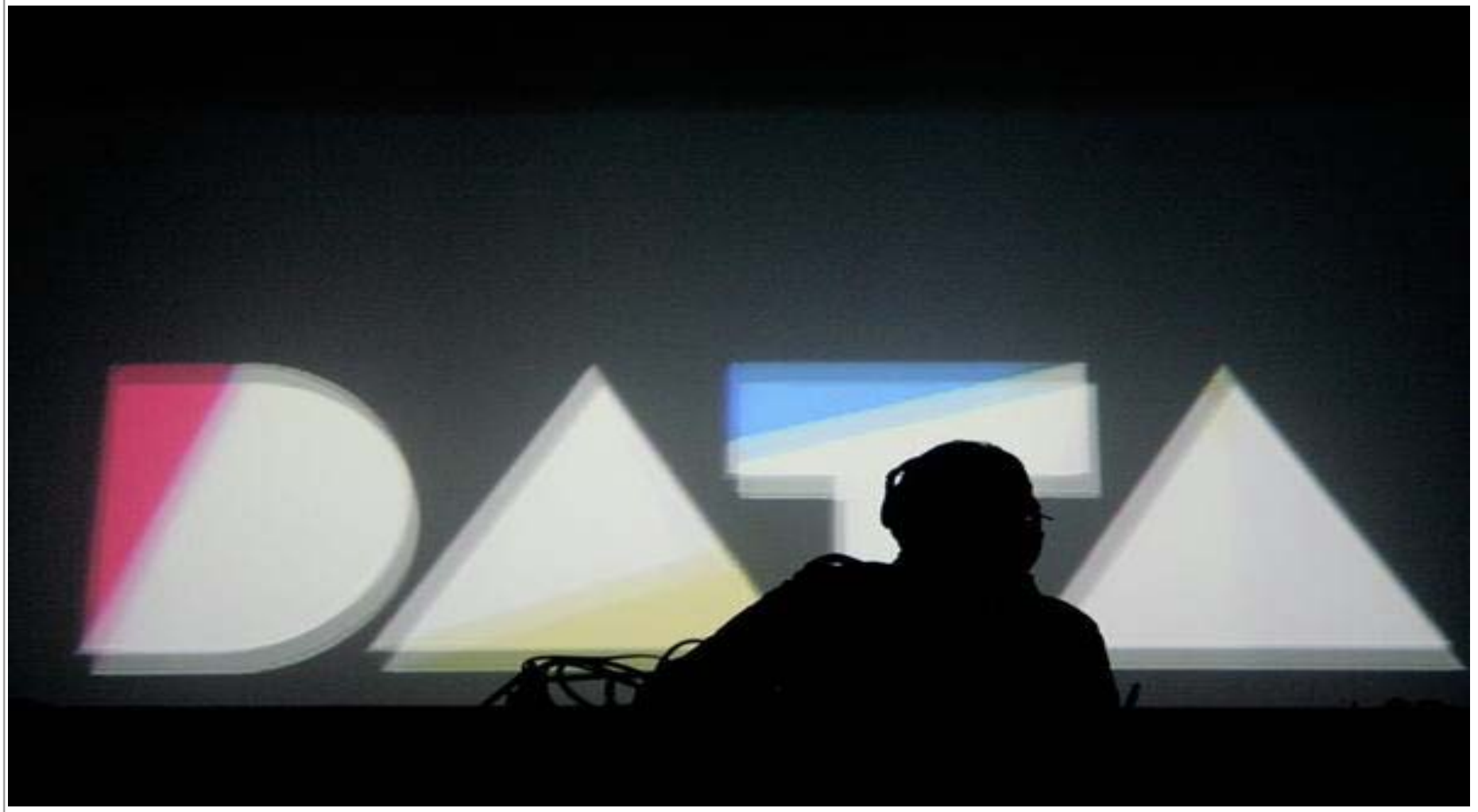
Cignet's penalty stems from failure to give 41 patients access to their medical records when they were requested, followed by a failure to cooperate with an investigation into the matter by the HHS Office of Civil Rights.

The Mass. General settlement arises from the loss of documents containing the protected health information of 192 patients. An employee accidentally left them on a subway, the story says.



THE UNIVERSITY of TEXAS SYSTEM  
*Nine Universities. Six Health Institutions. Unlimited Possibilities.*

# Am I a Data Owner?





# How Do I Know?

## The Role of Data Owner is defined in two places:

- Texas Administrative Code, Title 1, Part 10, §202.75 (TAC 202.75)
- The U. T. System Information Resources Use and Security Policy (UTS-165)  
(Refer to page 2 of the *Information Owner's Guide to Data Protection*.)

## Here are some hints:

- Are you a principal investigator for a research project?
- Are you an administrator in charge of a business function?
- Are you a faculty member who maintains a grade book?
- Do you have one of the following titles: Dean, Chairman, Director, Manager, Coordinator, etc.

**In doubt? Contact your Information Security Officer!**



# Information Security Roles

## Information Security Administrator (ISA)

- You appoint this person to assist with security tasks and as a liaison with the ISO.

## Data Owner (you)

## Information Security Officer (CISO or ISO)

- Administers the security program.
- The ISO is your resource – get to know this person.

Central IT

## Custodian

- Custodians provide IT services to you.
- They implement the controls that you specify.

3<sup>rd</sup> Party Outsourcer

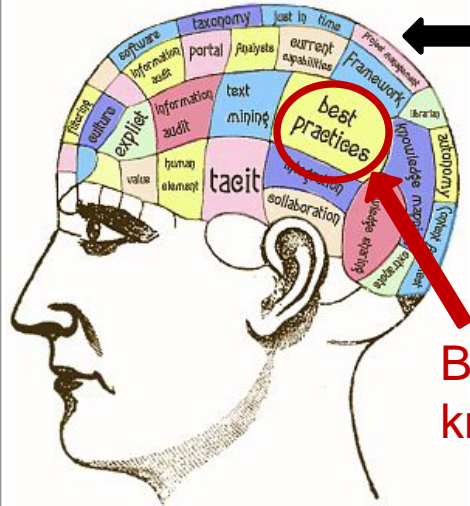
## Users

- You set the rules as to which users can access data and what they can do with the data.





# As an Owner, What do I Need to Know?



You do NOT need to know all of this.

But you do need to know some of these.

- Know your Information Security Officer.
- Know your Data Custodians.

- Know your Data.
- Know who has access to the Data.
- Know where your Data is located.
- Know how your Data flows – Where does it come from? Where does it go? When is it no longer needed?
- Know your applications and their capabilities.
- Know what controls are in place to protect your data.

## As an Owner, What Should I Do?

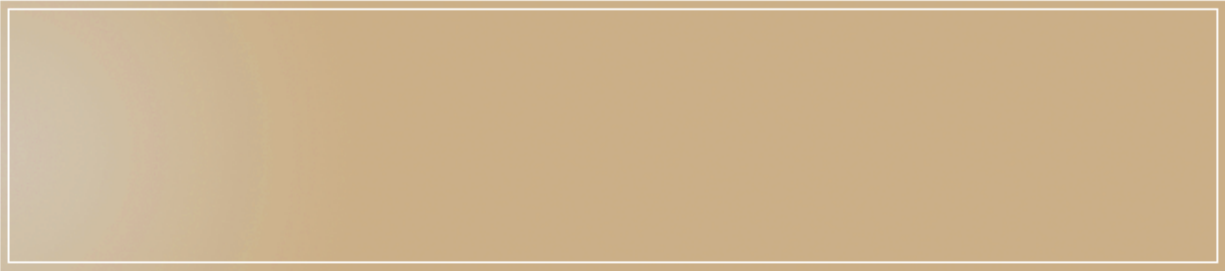
1. **Set an Example – This is Job One! You set the tone!**
2. Obtain a copy of the *Information Owners Guide to Data Protection*.
3. Appoint an Information Security Administrator.
4. Meet with your CISO/ISO to discuss your information security needs.
5. It's inventory time! Data, Servers, Applications, Contracts, Custodians.
6. Classify your Data.
7. Establish Data Access Policies.
8. Specify Security Controls and Select Custodians.
9. Perform a Risk Assessment.
10. Periodically Confirm that Controls Remain in Place!



Data Ownership is like Home Ownership. It requires constant maintenance.



THE UNIVERSITY of TEXAS SYSTEM  
*Nine Universities. Six Health Institutions. Unlimited Possibilities.*



THE UNIVERSITY OF TEXAS SYSTEMWIDE COMPLIANCE OFFICE



SYSTEMWIDE COMPLIANCE ACADEMY

PROVIDING COMPLIANCE LEADERSHIP AND GUIDANCE TO THE UNIVERSITY OF TEXAS SYSTEM

Lewis Watkins, CISO  
[lwatkins@utsystem.edu](mailto:lwatkins@utsystem.edu)

# Questions?