

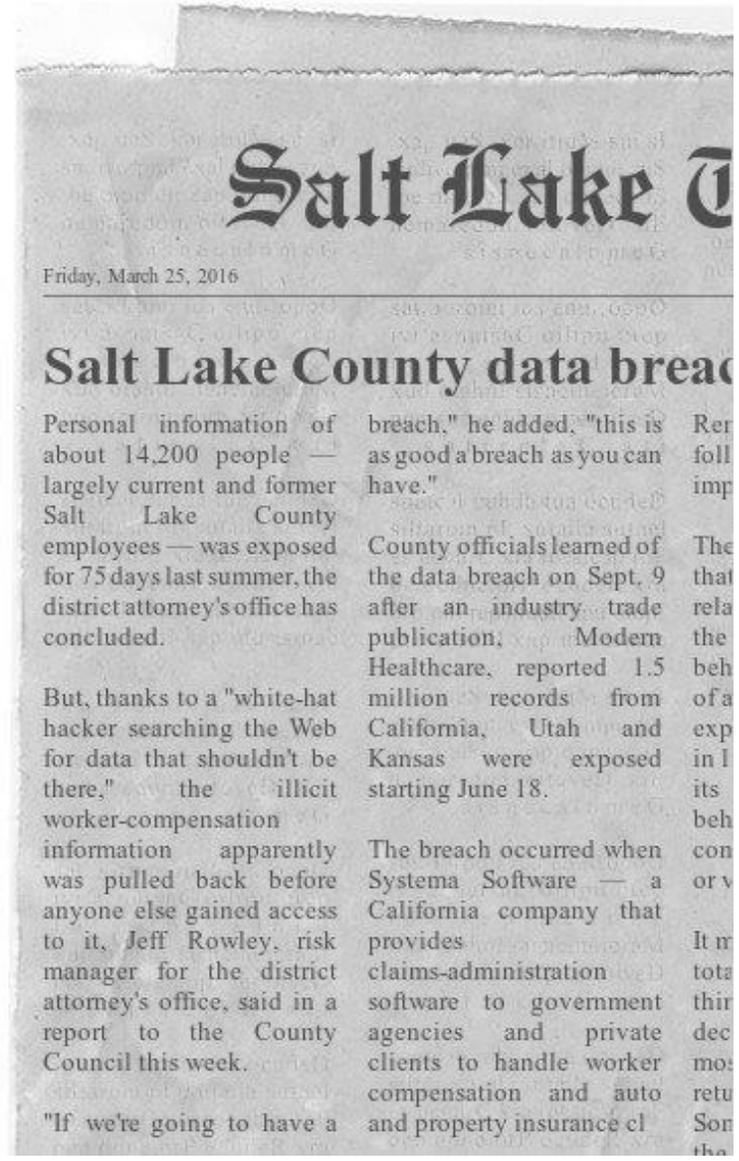
# DATA BREACHES ∞ CYBER SECURITY ARE YOU PREPARED?

Presentation By:

Valerie M. Wilde, Division Administrator  
Salt Lake County District Attorney's Office



September 9, 2015



# Salt Lake County's Data Breach

- Notification of the breach
- Is this a hoax?
- What is a white hat hacker?
- Understanding the loss and securing the data
- Notifying affected parties
- Addressing the Press and GRAMA requests
- Multi-state reporting
- Credit monitoring services
- Silence



# Financial costs

- Hundreds of staff hours
- \$99,615.00 without staffing costs (\$100,000 deductible)
  - Outside counsel
  - Outside PR firm experienced in responding to data breaches
  - IDT 911, plus additional credit monitoring
- Fully reimbursed by our outside vendor who handled the data



IS YOUR ORGANIZATION A SITTING DUCK OR  
CAN SOMETHING BE DONE TO PREPARE?



# Understand your data storage



- Think about the systems you use. Is your data contained within your county on your own servers? Or do you allow third party hosting of data?
- Do you host data in the cloud or have third party storage of data?
- Do you use any internet based databases?
- If you have external data, do you have up to date contact information for these service providers?
- Do your third party providers have strict security requirements for securing your data?

A screenshot of a Windows Explorer window showing a file folder structure. The window title is "Kali Linux" and the address bar shows "C:\Users\kali\Documents". The left pane shows a tree view of folders including "Documents", "Downloads", "Music", "Pictures", "Videos", and "Public". The right pane shows a list of files and folders with columns for Name, Date modified, Type, and Size. The files listed include "Documents", "Downloads", "Music", "Pictures", "Videos", and "Public".

Name	Date modified	Type	Size
Documents	11/11/2014	Folder	0 KB
Downloads	11/11/2014	Folder	0 KB
Music	11/11/2014	Folder	0 KB
Pictures	11/11/2014	Folder	0 KB
Videos	11/11/2014	Folder	0 KB
Public	11/11/2014	Folder	0 KB

# Understand the type of data you maintain

- The law categorizes information into PII (Personal Identifying Information) and PHI (Personal Health Information) and HIPPA covered Information.
- Different regulations apply to each category of information
- State Laws (Utah)
  - Utah Code Ann. 13-44-101 et seq. (Protection of Personal Information Act)
  - Utah Code Ann. 26-33a-101 (Utah Health Data Authority Act)
- Federal Laws
  - HIPPA HITECH, Privacy and Security Rules (45 CFR 160)



# PII (Personal Identifying Information)

- PII relevant to a breach in Utah includes an individual's name with one or more of the following:
  - Social Security Number
  - Driver license or state issues identification card number
  - Account number or credit or debit card number in combination any security code, access code or password, etc. permitting access to the person's account.
- Data owners are responsible for breach reporting and notifications
- Limited methods of notification delivery
- You must notify the UT Data Owner immediately if breached
- Violations can result in heavy fines
- Data protection laws extend out-of-state
- See Utah Code Ann. 13-44-101 et seq. (Protection of Personal Information Act)

# What is PHI (protected health information)?

- **Protected health information (PHI)** under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" and can be linked to a specific individual. This includes any part of a patient's medical record or payment history.
- Counties may have this information as it relates to services performed by their :
  - Health Department
  - Jail
  - County employees through their medical programs or Human resources
  - Other insurance programs (workers comp, life insurance, extended benefits)

# PROTECTED HEALTH INFORMATION (PHI) INCLUDES THE FOLLOWING TYPES OF DATA:

- Name, social security, driver's license or ID number
- Phone number, fax number, email, URL or other web addresses
- Medical record numbers, account numbers, policy numbers
- Serial numbers, vehicle numbers,
- Biometric identifiers, fingerprints, retinal or voice prints
- Full face photographs or other comparable images

# Under Utah law, there is no private right of action :

In Utah, the Attorney General enforces the law. There is no private right of action. Violation penalties could be up to \$2,500 per consumer, but not over \$100,000. The attorney general can seek injunctive relief to prevent future violations.

However, you may get direct claims relating to actual damages experienced by those persons involved in the data breach.

# If a breach occurs, what Action is required:

- **Secure your data and begin documenting the event**
  - Documentation will be key to any loss recovery, insurance company demands and responding to media
- **Understand the extent and manner of the data loss**
  - In order to properly notify, you need to know what was lost.
- **Notification**

After a determination regarding the scope of the breach and once reasonable integrity is restored to the system, the notification must be made in the most expedient time possible without unreasonable delay. An exception for delay is made if law enforcement indicates the notification may interfere with an investigation.

  - Be aware that other states use a different standard (risk of harm analysis). If there is a reasonable likelihood of harm then notification is required.

# Additional steps:

- Responding to media and notified parties
- Offering services to those impacted by the data breach
- Making necessary changes to regular operations
- Determining the financial impact from the breach
- Making a claim for any financial loss



# HIPPA COVERED DATA

- If your system contains Hippa data covered under the HIPPA HITECH Security Rules reporting must follow the federal rules. (45 CFR 160)
- Notification will need to be made under the rules, which also requires notification to the U.S. Department of Health and Human Services.
- Timeline for notification
- Plan for data post-Breach



## PENALTIES



Under HIPAA the Recovery Act allows for civil penalties of \$50,000 per violation, with a cap of \$1.5 million per calendar year for the most severe situations of willful neglect that a organization does not correct. The Office for Civil Rights (OCR) enforces complaints related to health information privacy and security.

# The Security Rule?

## Who needs to comply?

All HIPAA-covered entities and business associates of covered entities must comply with the Security Rule requirements.

The Security Rule does not apply to PHI transmitted orally or on paper.

## PHI vs. ePHI

Electronic PHI (ePHI) is classified as all PHI that is stored, transmitted, or used electronically.

## Secure What Info?

- Data in motion—data moving through a network (e.g., e-mail).
- Data at rest—data that is kept in databases, servers, flash drives, etc.
- Data in use—data that is in the process of being created, retrieved, updated, or deleted.
- Data disposed—data that has been discarded.

# So What can I do?

- Plan for a data breach
  - Have a response team ready
  - Understand your data and data storage systems
  - Know your reporting responsibilities
  - Consider additional insurance coverage options
- Discover and Investigate all breaches of data
  - Secure your data and report the breach
  - Send notification to impacted persons
  - Offer identity theft protection
- Make a public announcement and respond to news media
- Respond to inquiries
- Resume Business



# Other Resources:

- **Data Breach Response Guide** <http://www.experian.com/assets/data-breach/brochures/response-guide.pdf> (Experian Data Breach Resolution Team)
- Here is a 30-page PDF that includes how to handle each step of the response process, as well as information about specific kinds of breaches such as healthcare breaches.
- **Model Data Security Breach Preparedness Guide** (American Bar Association)  
[http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac\\_2012/22-15\\_intro\\_to\\_data\\_security\\_breach\\_preparedness.authcheckdam.pdf](http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/22-15_intro_to_data_security_breach_preparedness.authcheckdam.pdf)
  - This PDF provides an overview from the legal perspective of how to prepare for a data breach.
- **Data Breach Charts**
  - [http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data\\_Breach\\_Charts.pdf](http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf)
  - This is a great starting point to review how different states' data breach laws compare. Again, it doesn't take the place of your legal team, but it's a helpful overview.

# Cyber liability insurance

- Coverage can provide:
  - Damages related to cyber losses
  - Breach Council
  - Credit monitoring services
  - Assistance with meeting notification requirements in all 50 states
  - Counsel related to Press inquiries
  - Assistance with Follow up issues related to data retrieval

# The quiet end to a data breach

