HEALTH IT IN DISASTER RECOVERY

Presenter: Alaina Lamphear

HEALTH IT IN DISASTER RECOVERY AGENDA

- Introduction
- About Disaster Recovery Plans
- Real Life Disaster Examples
- Electronic Health Records and Natural Disasters
- IT Disaster Recovery Plans
- Cybersecurity in Natural Disasters
- Know your HER
- HIPAA and Natural Disasters
- HIPAA Breaches: A Disaster of Another Kind

PREPARATION

1994 Northridge Earthquake

It is the organization's preparedness and ability to respond and restore its systems and operations that make the difference between an extremely strenuous event that will have long-term effects and a dodged bullet.

DISASTER RECOVERY PLANS

- Why the need to implement a Disaster Recovery Plan?
- Why is there the need to implement HIT into the DRP?

REAL-LIFE EXAMPLES
AND ALL AROUND

- Fires
- Earthquakes
- Tsunamis
- Power Outages
- Cyberattacks

Is your organization prepared?

CAMP FIRE

- Paradise, California
- November 2018
- 86 people killed
- 153,000 acres burned
- 14,000 residences destroyed
- Paradise lost 90% of its population after the fire
- Claimed nearly three times as many lives and structures than any other wildfire in California's history

CAMP FIRE

6:30 AM

- Reports of a small fire came in (November 8)

9:00 AM

- Fire was estimated at 2,500 acres

1:00 PM

- 8,000 acres
- Quickly grew to 20,000 acres hours later

The fire grew at ***80 football fields per minute!!!***

CAMP FIRE

- East Avenue Church in Chico was designated a clinic
- Tended to 300 patients
- Among 240 patients served at pop-up disaster clinic shortly after the fire, all identified as low income
  - 60% suffered chronic illness
  - 35% were diagnosed with a mental health condition
  - Over 30% were uninsured
  - 40% noted that they were without regular medical care
- The homes of roughly 75% of the staff and doctors had perished in the blaze

CAMP FIRE: AFTER DISASTER

CAMP FIRE: BEFORE DISASTER

HURRICANE KATRINA

- New Orleans, Louisiana
- August 2005
- 1,200 people killed
- Cat 3 storm with winds reaching speeds as high as 120 miles per hour
- Costliest storm in US history ($108 billion in property damage)
- Many patient records were physically destroyed during Hurricane Katrina
  - Still many paper records as EHRs were not fully adopted

HURRICANE KATRINA

- Photo: Galveston, Texas
- Alexa Cross experienced:
  - Hurricane Ike (2008)
  - Tropical Storm Allison (2001)
  - Hurricane Harvey (2017)

ELECTRONIC HEALTH RECORDS

Today nearly all healthcare facilities use EHRs

- Widespread EHR adoption and use better equips healthcare systems for quick response to emergency events
- Hurricane Harvey in Houston, Texas
  - Hospitals affected by flooding could continue operations
- EHR accessibility
  - Remotely backed up and remote/mobile applications
- Provider confidence
  - Accessibility
  - Adoption

DISASTER SCENARIO: TORNADO

- Manhattan, Kansas
- June 2008
- EF4 Tornado
- Chief Operations Officer's home took a direct hit
- Just returned home, with no time to prepare
- Laptop was found in the yard, wide open, and still (somewhat) functioning

IT DISASTER RECOVERY PLANS

- **Where do you keep your current management plan?**
  - Hard copy
  - Locally stored (computer, server, etc)
  - Thumb drive
  - Cloud storage
- **Can you access manual?**
  - Without a computer
  - If the power is out for an extended amount of time
  - If location where manual is stored is inaccessible
  - Without an internet/WiFi connection
  - On your phone or other mobile device

IT DISASTER RECOVERY PLANS

- **Who has access to your emergency manuals?**
  - All leadership/essential management should have a copy/access

Tips to remember:

- Utilize free tools, like Google Docs
  - Cloud storage
  - Accessible to all
- Print, laminate and keep with your home, work and car emergency kits a list of:
  - Important organization contacts
  - Web addresses (such as EHR remote address)
  - Immediate disaster protocol
- Provide two copies of manuals to all leadership
- Consider keeping an encrypted copy of plans with a trusted third party, like CCALAC

CYBERSECURITY AND DISASTER RECOVERY

- **Do you have an IT recovery plan in place?**
  - Designated primary and secondary contacts
  - Where is the list of important vendor contacts stored?
  - Who has responsibility for any hardware that may need moved/removed?
- **How do you host your EHR?**
  - Local hosted (ie: server on site)
    - Multiple levels of security
    - Located in a disaster secure location
    - What is your backup cadence?
  - Cloud hosted
    - What is the backup cadence?
    - How will you access if no internet/power
  - What are the locations of the data centers? How many data centers contain backup?

CYBERSECURITY AND DISASTER RECOVERY

- **Multi-Factor Authentication**
  - Technology that can access PHI remotely has multi-factor authentication
    - We use DUO at DataFile
- **Password security**
  - Secure passwords so they are inaccessible to others
    - Password keeper on your phone
  - Do not write password on the outside of the thumb drive
- **Network security**
  - Only access PHI through secure, password protected network
  - Do not give the password to anyone but essential employees
  - WiFi hotspot on phones
  - VPN when accessing PHI
  - Closed network only

KNOW YOUR EHR

- **Petaluma Health Center and eClinicalWorks**
  - eClinicalWorks campaign feature
    - Allows mass messaging to a group based on your defined parameters
  - Encourage patient portal adoption
  - Know your mobile capabilities (like eClinicalTouch) and train at least two providers in usage
  - Utilize ePrescribe functions
  - Utilize a business associate who understands your organization and your EHR to allow for unexpected changes in patient volume
    - If clinic is closed:
      - Medical records can still be transferred
      - Incoming documents can still be processed
    - If the clinic is open:
      - Influx of patients needing treatment, transferring records, etc. from other clinics

HIPAA AND NATURAL DISASTERS

- **Is the HIPAA Privacy Rule "waived" or "suspended" during an emergency?**
  - Generally no, unless there is an exception by the US Secretary of Health and Human Services AND:
    - A public health emergency is declared AND
    - The President declares an emergency or disaster under the Stafford or National Emergencies Act
- **How does the HIPAA Privacy Rule apply to us in a disaster?**
  - Even WITHOUT a disaster waiver – patient information can be shared under certain conditions and for certain purposes such as:
    - Treatment (as necessary to treat a patient or another person)
    - Public health activities
    - To persons at risk

Source: https://www.hhs.gov/sites/default/files/hurricane-irma-hipaa-bulletin.pdf

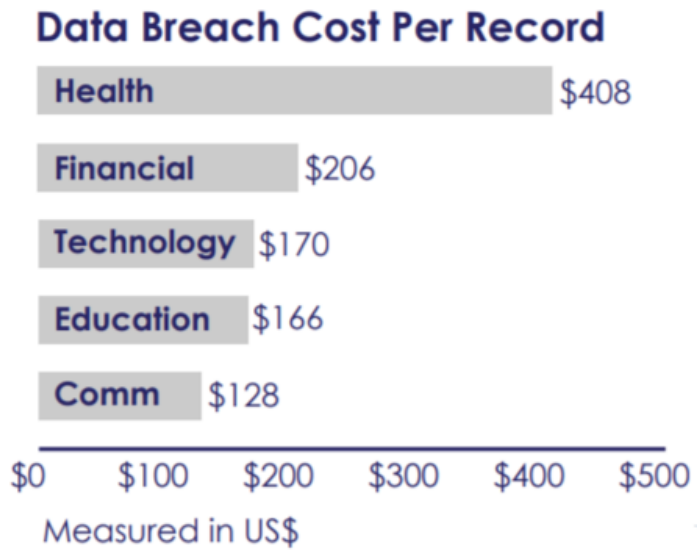
CYBER ATTACKS:
A DISASTER OF A DIFFERENT KIND

- Unauthorized disclosure
- Ransomware
- Phishing
- Unauthorized access

CYBER ATTACKS: WHY HEALTHCARE?

- **HHS has stated that healthcare data breaches have the highest cost per record.**
  - $408 per record cost

- **Possible reasons a healthcare record is worth more:**
  - Healthcare data race
  - Insurance costs
  - Late technology adopters



CYBER ATTACKS: UNAUTHORIZED DISCLOSURE

- **What is an Unauthorized Disclosure?**
  - An unauthorized disclosure occurs anytime PHI is disclosed to someone who is not authorized to received the information.
  - Different types including:
    - Miskey of the fax number
    - Incorrect email address
    - Theft or loss of device
- **Unauthorized disclosure is the most common type of breach/violation**

CYBER ATTACKS: UNAUTHORIZED DISCLOSURE

- **How can I prevent these incidents?**
  - Incorrect email address:
    - Is your organization using an encryption software, like Zix?
  - Theft or loss of device:
    - Password security
    - Sensitive information or PHI should not be saved to the hard drive
    - Two-factor authentication
    - Do not save passwords in browser
    - Review basic security with your staff
    - Always lock your computer

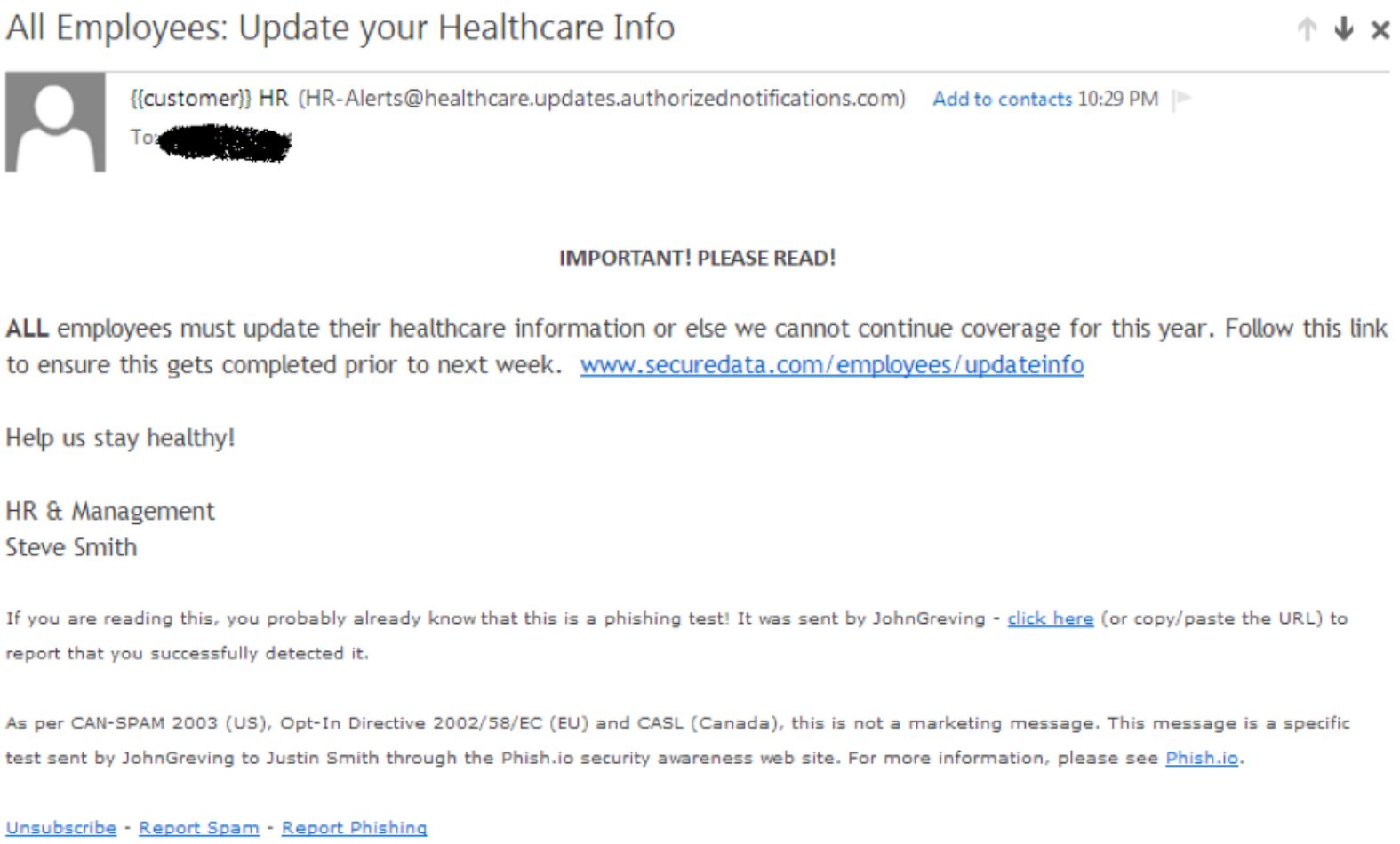
CYBER ATTACKS: RANSOMWARE

- **What is Ransomware?**
  - Malicious software that takes over your computer and makes it unable to use, demanding money to unlock.
    - Several types of Malware:
      - Ones that lock or encrypt your system
      - Those that model themselves as fake virus software
      - Mobile device specific items
    - Example: https://www.youtube.com/watch?v=NJGyTiEBDZY
- **Why would they target us – we are small!**
  - In October 2019, the largest recorded HIPAA breach as to a CHC
    - Betty Jean Kerr People's Health Center – St. Louis, Missouri
    - 152,000 records affected
    - Hackers target those that are perceived to have a smaller IT Security team

CYBER ATTACKS: PHISHING

- **What is Phishing?**
  - The act of sending fraudulent emails appearing to be from reputable people/companies in order to gain access to passwords, logins, other information.
  - Different types including:
    - Spear Phishing
    - Whaling
- **Phishing emails can lead to a larger, more intrusive problem such as Malware.**
- **Prevention is key!**
  - Do you have a spam block/firewall in place to quarantine questionable emails?
  - Is your staff properly trained in recognizing key elements to identify phishing emails/websites?
  - Require staff to utilize their organization's email for all correspondence – especially that of which includes items of a sensitive or protected nature.

CYBER ATTACKS: PHISHING EXAMPLES



All Employees: Update your Healthcare Info

{{customer}} HR (HR-Alerts@healthcare.updates.authorizednotifications.com) Add to contacts 10:29 PM

To: [redacted]

IMPORTANT! PLEASE READ!

ALL employees must update their healthcare information or else we cannot continue coverage for this year. Follow this link to ensure this gets completed prior to next week. www.securedata.com/employees/updateinfo

Help us stay healthy!

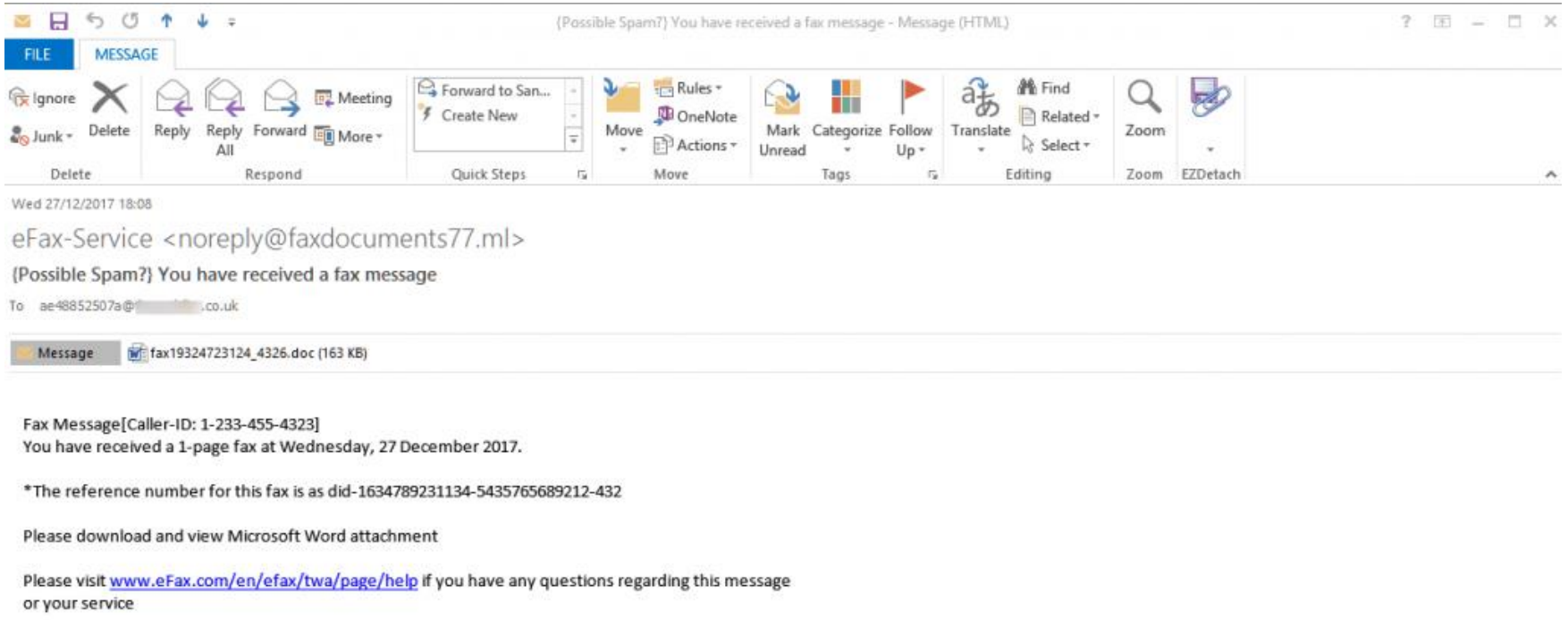
HR & Management
Steve Smith

If you are reading this, you probably already know that this is a phishing test! It was sent by JohnGreving - click here (or copy/paste the URL) to report that you successfully detected it.

As per CAN-SPAM 2003 (US), Opt-In Directive 2002/58/EC (EU) and CASL (Canada), this is not a marketing message. This message is a specific test sent by JohnGreving to Justin Smith through the Phish.io security awareness web site. For more information, please see Phish.io.

Unsubscribe - Report Spam - Report Phishing

CYBER ATTACKS: PHISHING EXAMPLES



CYBER ATTACKS: UNAUTHORIZED ACCESS

- **What is Unauthorized Access?**
  - Access of anyone who is not authorized to be in the system.
- **Types of Unauthorized Access:**
  - Employees that are no longer actively employed
  - Computers being left unlocked
  - Unsecure password storage
  - PHI stored unsecurely

CYBER ATTACKS: UNAUTHORIZED ACCESS

- **How to prevent unauthorized access:**
  - If employee is terminated/no longer with the organization
    - Deactivate all accounts related to them – including emails
    - If it's not possible to deactivate the accounts – change all passwords to something that has not been utilized/known by the former employee
    - Require all employees to provide a list of places they may utilize unique credentials, for business purposes, to make things easier when updating all accounts.
    - Keep the above lists of information in a secure vault/password state based on role/department so the tools are ready in the case of employee termination.
    - Remove all applications from employee's personal mobile device.

CYBER ATTACKS: UNAUTHORIZED ACCESS

- **How to prevent unauthorized access:**
  - Computers are left unlocked/passwords are left in unsecure locations
    - Regular PHI/security sweeps
    - Demonstrations – how quickly someone could access an unlocked computer
    - Pushing mandatory autolocking of computers to all systems after a brief amount of time
    - Create a safety culture
  - PHI stored unsecurely
    - Provide locked storage for any paper records
    - PHI/security sweeps
    - Regular PHI checks within shared drives
    - Limit access to EHR
    - Unique logins