HIPAA PASS

Privacy and Security Solutions

Tabletop exercise
Cyber security attack response

mountain-pacific quality health
HEALTH TECHNOLOGY SERVICES
transforming health care through innovative technology

Legal Disclaimer

The presenter is not an attorney and the information provided is the presenter(s)' opinion and should not be taken as legal advice. The information is presented for informational purposes only.

Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar(s) and related materials (including, but not limited to, recordings, handouts, and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar(s) and webinar materials should not in any manner rely upon or construe the information as legal, or other professional advice. Users should seek the services of a competent legal or other professional before acting, or failing to act, based upon the information contained in the webinar(s) in order to ascertain what is may be best for the users individual needs.

Agenda

- Tabletop test
- How these affect you and your job
- What information must be protected
- How you can protect confidential and sensitive information
- Your responsibilities for good computer practices
- How to report privacy breaches and security incidents

What is a tabletop test?

- Real recovery: Cut-over systems, re-routing cloud based EHR, email, phones, staff relocation.
- Test recover: Cut-over of limited systems, relocating small team
- Individual system recovery: Full test recover and cut-over of critical systems
- Tabletop recovery test: Walk-through recovery without performing actions

What does it look like?

For today's boot camp:

- Facilitator will set the scene and describe series of hypothetical
- We all work for WeCureU Healthcare
- Audience will participate, there are no wrong answers
- Professional opinions
- Adapt and continue through plan to recovery

Follow-up at your facility:

- Follow up plan, what needs to be fixed?
- Distribute review material
- Carry out the actions
- Report to participants and other stakeholders
- Plan your next test

Please remember

- A tabletop test is not a replacement for technical testing
- Record and check all expectations (don’t assume)
- It’s only a failure if you don’t learn from the test so you can make improvements for next time.

Scenario #1

On June 30, 2018, at 9am, WeCureU Healthcare receives an email from an anonymous source that WeCureU has been a victim of a data breach, and that the health records (ePHI) of its patients are currently available on various Dark Net websites.

Do you think WeCureU Healthcare should investigate? If so, what are the steps?

Scenario #1
Feedback and Opinions

- Instigate to see incident, do not ignore
- Due care, do an initial investigation
- Don’t call it a breach yet, talk with IT Staff, can you identify the source
- Law enforcement or reputable company to check out Dark Net
- Not advisable to go on the Dark Net, very dangerous, several sites have malware and will infect you
- All incidents should be reported even if nothing

Scenario #2

On June 30, 2018, at 9am, WeCureU Healthcare receives an email from a known reporter stating that they have information from credible sources that WeCureU has been a victim of a data breach, and the health records (ePHI) of hundreds of its patients are currently available on various Dark Net websites. The reporter is looking for a comment from WeCureU and plans to report the story soon.

How should WeCureU respond to the report? What steps should WeCureU take?

Scenario #2
Feedback and Opinions

- Activated teams,
- Keep senior leadership/Board of Directors updated, about to have public relations crisis.
- Not saying no comment, saying cooperating with authorities.
- All groups need to work in tandem.
- Confirm, not deny, looking into the matter, no information at this time, working with authorities.
- Work with reporter, try to push their report date back, probe reporter for more information.
- If not successful see if reporter will give up the kind of source i.e. government, informed expert, foreign government.

Scenario #3

Same facts as Scenario #2. WeCure U Healthcare's internal investigation determines that a data breach has occurred. Our IT staff are unable to determine the cause or the scope of the breach. WeCureU's Incident Response Plan directs the CEO to retain outside cybersecurity consultant to conduct an investigation.

How should the engagement be structured?

What would be the impact if records were encrypted?

Scenario #3
Feedback and Opinions

- We are past the point of logs, need expert to install tools, special monitors, computer forensics i.e., cyber security firms
- Advance integration of the cyber response, incident response, breach notification (checklist important when hair is on fire)
- Breach notification to patient, federal, state and sometimes press
- Notify insurance company asap and get preapproved
- Retain more than one cyber security company, especially if using 0 dollar retainer
- Experts claim cyber attack can cost from $150,000 to $2 million
- Legal involved
- You are the victim, law enforcement will want to work with you

Scenario #4

Same facts as Scenario #2. WeCureU Healthcare’s security staff suggests contacting law enforcement.

Should WeCureU contact law enforcement?

What are the benefits and the cost of contracting law enforcement?

Scenario #4
Feedback and Opinions

- Is it too soon, haven’t completed our own investigation? Yes, to have a high-level conversation, free resources, Due care
- Will become public anyway, involve to help
- It is their investigation to handle, need to help them do their job, sometimes causes tension if investigation goes on, CEO wants it to be over

Scenario #5

Same facts as Scenario #3. The outside cybersecurity consultant has begun its investigation. However, before the consultant has been able to make any progress in its investigation the reporter issues his story concerning the data breach. As a result, patients begin contacting WeCureU Healthcare's security staff suggests contacting law enforcement.

How should WeCureU respond to inquires from patients?

What should it disclose at this point? What is required under the Breach Notification Rule?

What are WeCureU's additional responsibilities?

Scenario #5
Feedback and Opinions

- Breach notification under State and HIPAA
- Scripting, get in front of the communications to patients.
- Have a single message, not conflicting
- Don’t speculate, just in case you are wrong
- Make sure staff know **who** in the organization can talk to the press.

Scenario #6

- Same facts as #5, have determined malware in fishing email, from ecommerce server, what are the notifications requirements?

Scenario #6
Feedback and Opinions

- What state are they in, encrypted?
- Most States have data breach notification status. Who's data and what State statues apply
- Breach Notification under HIPAA and possible State Medical Information laws
- Notifications under PCI compliance, credit card industry
- Several different parties that you need to notify asap, nice to have checklists
- Consider any contractual obligation for disclosure

Scenario #7

Same as number 6, except only the information that was accessed and taken was not the Protected Health Care or ecommerce (credit card and payment) but instead employee records.

Does it make a difference if the affected users were employees.

Scenario #7
Feedback and Opinions

- Pretend employee records were encrypted
- Who do you notify?

Susan Clarke

Health Care Information Security and Privacy Practitioner

www.gotohts.org

cell: 307.248.8179

mountain-pacific quality health
HEALTH TECHNOLOGY SERVICES
transforming health care through innovative technology

HCISPP®