

# Ransomware and Breach

HHS Office for Civil Rights



## Agenda:

- Ransomware Prevention
- Ransomware Recovery
- Breach Review
- Ransomware and Security Incidents
- Ransomware and Breaches
- Breach Resources



#### Ransomware Prevention:

- Security awareness and training
  - Processes are in place to detect/guard against malicious software
  - Train workforce how to detect and report malicious software
- Risk analysis
  - Identify the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI entities create, receive, maintain, or transmit
- Risk management
  - Implement security measures sufficient to reduce identified threats and vulnerabilities to a reasonable and appropriate level
- Access controls
  - Ensure access rights granted are not excessive
- Business Associate Agreements
  - Define processes, including responsibilities, to prevent, manage and report security incidents and breaches



#### Ransomware Recovery:

- Security incident response
  - Prepare for security incidents ahead of time
    - Define teams and activities
  - Detect and conduct initial analysis of incident
    - Identify scope of incident
    - Determine origination (who/what/where/when)
    - Determine if incident has concluded or is ongoing
    - Determine how incident occurred
  - Contain the impact and propagation of the incident
  - Eradicate the incident and vulnerabilities which may have permitted its ingress and/or propagation
  - Recover from incident (restore lost data, return to business as usual)
  - Post-incident activities which could include responding to regulatory and/or contractual obligations as a result of breach



#### Ransomware Recovery:

- Contingency plans
  - Data backup plans
  - Disaster recovery plans
  - Emergency operations mode plans
  - Testing and revision procedures
    - Conduct test restorations to verify the integrity of backed up data and provide confidence in data restoration capabilities
    - Testing contingency plans to ensure organizational readiness and provide confidence that contingency plans would be effective
    - Revise contingency plans if tests show areas which would be ineffective
  - Application and data criticality analysis
    - Ensure all critical applications and data are accounted for as part of the contingency plans



#### Breach

The acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

### Presumption

The breach is <u>presumed</u> and requires notification to individuals and HHS (and to the media for large breaches) unless the entity demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment.



#### **Breach Risk Assessment:**

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.





### Security Incident:

- A security incident under the HIPAA Rules is "...the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." See 45 C.F.R. 164.304.
- The presence of ransomware on a covered entity's or business associate's computer systems is a security incident.
- If a ransomware attack is detected the affected entity should immediately activate its security incident response plan, which should include measures to isolate the infected computer systems in order to halt propagation of the attack.



### Breach:

- A breach under the HIPAA Rules is "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."
- When ePHI is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule.



#### **Breach Notification:**

- Unless the covered entity or business associate can demonstrate that there is a "…low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred.
- The entity must then comply with the applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements. See 45 C.F.R. 164.400-414



Ransomware Guidance

http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Breach Notification/Reporting Resources

http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

https://ocrportal.hhs.gov/ocr/breach/wizard\_breach.jsf?faces-redirect=true