HIPAA Security Rule
Complying with the Requirements for Contingency Planning

NIST/OCR Safeguarding Health Information Conference
May 12, 2010

David Holtzman, J.D.
Health Information Privacy Division, Office for Civil Rights
Contingency Plan Standard
45 CFR 164.308(a)(7)

- Security Rule standard requires that a covered entity establish and implement policies and procedures for responding to an emergency that damages systems that contain ePHI
  - Fire or Theft
  - Vandalism
  - Natural Disaster
  - System Failure
Contingency Plan Standard
45 CFR 164.308(a)(7)

- Creating and testing plans for emergencies
  - Are physical and technical safeguards for EPHI built into contingency plans?
  - Are processes in place to incorporate system modifications into plans?
  - Are all information systems and peripherals identified and incorporated into emergency planning and testing?

- Related to Contingency Operations and Emergency Access Procedures
Implementation Specifications
Data Backup & Disaster Recovery Plans

- **Data Backup Plan (Required)** – Policies and procedures for creating and storing electronic media
  - Are systems that store EPHI preserved to backup media on a regular basis?
  - Are procedures in place to safeguard EPHI stored on backup media?

- **Disaster Recovery Plan (Required)** – Is there advance planning to recover system information after catastrophic loss
  - Are components of disaster recovery plan periodically tested and updated?
Emergency Mode Operation Plan (Required)
- Policies and procedures for the continuity of operations
  • Are security measures for critical business functions identified and incorporated into emergency operation plans?

Testing and Revision Procedures (Addressable) – Appropriate level of testing and revision of business contingency plans
  • Are periodic contingency plan exercises of performed and documented?
Applications and Data Criticality Analysis (Addressable) – Has there been appropriate consideration given classification of information system assets supporting critical business functions

- Are all information systems that access, transfer, or store EPHI identified and documented?
- Are all information systems that access, transfer, or store EPHI classified according to priority for contingency operations?
Want More Information?

The OCR website, [http://www.hhs.gov/ocr/privacy/](http://www.hhs.gov/ocr/privacy/) offers a wide range of helpful information about health information privacy including educational information, FAQ’s, rule text and guidance for the Privacy, Security, and Breach Notification Rules.