

SECURITY RULE

Effective April 20, 2005

Applies to electronic PHI (“EPHI”) only – defined as “health information maintained or transmitted by a Covered Entity (CE) in electronic form” – requires administrative, physical and technical safeguards

Main points:

- Scalability – may scale methods of compliance to the size of the CE
- Comprehensiveness – entire CE and entire workforce
- Technology neutral – no specific technology required; **each CE must choose what to implement**
- Internal and external security threats – CE must protect EPHI against internal and external threats
- Risk analysis – regularly conducted

Key concepts:

- Principle-based – NOTE: **there is no step-by-step checklist provided in the Rule**
- Reasonable – “reasonably anticipated” risks to EPHI must be mitigated
- Full compliance – includes at-home and all other workers
- Documentation – document and approve security processes/policies/procedures
- Ongoing – regular training of workforce; revise programs as needed

Administrative safeguards:

- Security management – policies to prevent, detect, contain and correct security violations; risk analysis, risk management, and sanction/security policies
- Assigned responsibility – a single individual must have responsibility, assigned in writing, for the overall security of a CE’s EPHI
- Workforce security – only authorized staff may have access to EPHI
- Information access – policies for authorizing, establishing and modifying access to EPHI
- Security awareness/training – program for entire workforce developed and maintained
- Security incident procedures – program to report, respond to and manage security incidents
- Contingency plan – for response to disaster/emergency that damages information systems containing EPHI
- Evaluation – periodically determine the extent that CE’s security policies meet the ongoing requirements of the Rule
- BAA – must say that BA’s will adequately safeguard the EPHI

Physical safeguards:

- Facility access – limit physical access to EPHI
- Workstation use – policy must specify the use of workstations and the characteristics of the physical environment of workstations that can access EPHI
- Workstation security – physical safeguards and limit only to authorized users
- Device and media controls – for receipt and removal of hardware and electronic media containing PHI

Technical safeguards:

- Access control – for systems containing EPHI (to allow access only to authorized persons)
- Audit controls – to record and examine activity within systems
- Integrity – to protect EPHI from improper modification/destruction
- Person/entity authentication – to verify that persons/entities seeking access to EPHI are who they claim to be
- Transmission security – to prevent unauthorized access to EPHI that is transmitted over an electronic network (i.e., the Internet or an Intranet)