

Required Security Procedures for Electronic Health Information

<u>Requirement</u>	<u>Implementation</u>
1. Certification	Security evaluation of computer systems (performed internally or by an external accrediting agency)
2. Chain of trust partner agreement	Contracts with clearinghouses and other agents ensuring security at all links in the data chain
3. Contingency plan	Data backup, disaster recovery, emergency access and operation
4. Formal mechanism for processing records	Documented policies and procedures for maintaining security, data authentication
5. Information access control	Access authorization, establishment and modification, encryption
6. Internal audit	Audit trails, alarms and schedule for on-going review
7. Personnel security	Security responsibility assigned to specific individual, background checks and clearance procedures
8. Security configuration management	Hardware/software installation, maintenance, testing, workstation security and log-on/off procedures, virus checking
9. Security incident procedures	Reporting and responding to security breaches
10. Security management process	Risk analysis and management, sanctions
11. Termination procedures	Removal from access, turn-in/change keys, cards and passwords
12. Training	Awareness training for all personnel, including management, reminders

© 2000 Scott C. Withrow. All rights reserved.

NOTE: This site includes a summary of certain compliance issues facing healthcare providers today. This site does not, and is not intended to, give legal advice. Reference should be made to full text of the statutes and regulations for complete analysis. Consultation with competent counsel is strongly recommended.