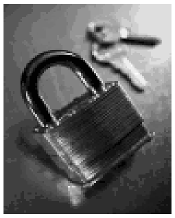
HIPAA Security Checklist



By Leigh-Ann M. Patterson, Esq.
Nixon Peabody LLP, Partner, HIPAA Task Force

I. Security Goals

- ☐ Ensure Confidentiality, Integrity and Availability of PHI
- ☐ Protect Against Threats
- ☐ Protect Against Anticipated Uses and Disclosures
- ☐ Ensure Compliance by Workforce

II. First Safeguard: Administrative Safeguards

Nine Security Standards:

1. **Security Management Process**
   - ☐ Risk Analysis (Required)
   - ☐ Risk Management (Required)
   - ☐ Sanction Policy (Required)
   - ☐ Information System Activity Review (Required)

2. **Assigned Security Responsibility**
   - ☐ Designate Security Officer (Required)

3. **Assigned Workforce Security**
   - ☐ Authorization and/or Supervision (Addressable)
   - ☐ Workforce Clearance Procedures (Addressable)
   - ☐ Termination Procedures (Addressable)

4. **Information Access Management**
   - ☐ Isolating Healthcare Clearinghouse Functions (Required)
   - ☐ Access Authorization (Addressable)
   - ☐ Access Establishment and Modification (Addressable)

5. **Security Awareness Training**
   - ☐ Security Reminders (Addressable)
   - ☐ Protections From Malicious Software (Addressable)
   - ☐ Log-in Monitoring (Addressable)
   - ☐ Password Management (Addressable)

6. Security Incident Procedures

- ☐ Response and Reporting (Required)

7. Contingency Plan

- ☐ Data Backup Plan (Required)
- ☐ Disaster Recovery Plan (Required)
- ☐ Emergency Mode Operation Plan (Required)
- ☐ Testing and Revision Procedures (Addressable)
- ☐ Applications and Data Criticality Analysis (Addressable)

8. Evaluation

- ☐ Periodic Technical and Non-Technical Evaluation (Required)

9. Business Associate Contracts

- ☐ Enter Into Business Associate Contract (Required)

III. Second Safeguard: Physical Safeguards

Four Security Standards:

10. Facility Access Controls

- ☐ Contingency Operations (Addressable)
- ☐ Facility Security Plan (Addressable)
- ☐ Access Control and Validation Procedures (Addressable)
- ☐ Maintenance Records (Addressable)

11. Workstations Use

- ☐ Proper Functioning and Physical Attributes of Workstations (Required)

12. Workstations Security

- ☐ Physical Safeguards to Restrict Access to Authorized Users (Required)

13. Device and Media Controls

- ☐ Proper Disposal of PHI and hard/software storing PHI (Required)
- ☐ Media Re-Use (Required)
- ☐ Accountability (Addressable)
- ☐ Data Backup and Storage (Addressable)

IV. Third Safeguard: Technical Safeguards

Five Security Standards:

14. Access Controls

- ☐ Unique User Identification (Required)
- ☐ Emergency Access Procedure (Required)
- ☐ Automatic Logoff (Addressable)
- ☐ Encryption (Addressable)

15. Audit Controls

☐ Record Internal Uses of PHI by User (Required)

16. Integrity

☐ Mechanism to Authenticate Electronic PHI (Addressable)

17. Person or Entity Authentication

☐ Person/Entity Seeking Access Is The One Claimed (Required)

18. Transmission Security

☐ Integrity Controls (Addressable)
☐ Encryption (Addressable)

V. Organizational Requirements

Two Security Standards:

19. Business Associate Contracts

☐ Business Associate Contracts (Required)

20. Group Health Plans

☐ Ensure Plan Documents Limit Plan Sponsor's Access to PHI (Required)

VI. Policies, Procedures and Documentation Requirements

Two Security Standards:

21. Policies and Procedures

☐ Reasonable and Appropriate Policies to Comply with Security Rule (Required)

22. Documentation

☐ Six-Year Time Limit (Required)
☐ Availability of Documentation (Required)
☐ Updates (Required)
☐ Encryption (Addressable)

About the author: **Leigh-Ann M. Patterson, Esq.,** is a partner in the law firm of Nixon Peabody LLP, where she focuses her practice on healthcare litigation, medical privacy issues and HIPAA compliance. Ms. Patterson founded Nixon Peabody's HIPAA Task Force Group in 2001. She may be reached at (617) 345-1258 or via e-mail at Lpatterson@nixonpeabody.com. *You are invited to contact Leigh-Ann via phone or email for free educational HIPAA resources, including free HIPAA articles and newsletters.* © 2003