White Paper on HIPAA Security
Surety Technologies, Inc.
January, 2012

HIPAA Compliance

There are two areas of compliance for HIPAA. The two areas are the Privacy Rule and the Security Rule. The Privacy Rule sets the standards for, among other things, who may have access to Protected Health Information (PHI), while the Security Rule sets the standards for ensuring that only those who should have access to Electronic Protected Health Information (ePHI) will actually have access.

The Privacy Rule applies to all forms of patients' protected health information, whether electronic, written, or oral. In contrast, the Security Rule covers only protected health information that is in **electronic** form. A health care provider is a covered entity if the person, business or agency furnishes, bills, or receives payment for health care in the normal course of business AND conducts those transactions electronically.

The Privacy Rule requires covered entities to have in place appropriate administrative, physical, and technical safeguards and to implement those safeguards reasonably. As a result, covered entities that have implemented the Security Rule requirements in their organizations will find that they have already taken many of the steps required for the Privacy rule and can apply those accordingly without duplication of effort.

For the small to mid-sized covered entity, the following Security rules need to be addressed. These codes are used in the descriptions to describe the level of discretion or judgment allowed for the covered entity:

(R) = Required - the covered entity must implement policies and/or procedures that meet what the implementation specification requires

(A) = Addressable - the covered entity must assess whether it is a reasonable and appropriate safeguard in the entity's environment. This involves analyzing the specification in reference to the likelihood of protecting the entity's EPHI from reasonably anticipated threats and hazards. If the covered entity chooses not to implement an addressable specification based on its assessment, it must document the reason and, if reasonable and appropriate, implement an equivalent alternative measure

HIPAA Security Rule Series

Administrative Safeguards

1. **Security Management Process:** Implement policies and procedures to prevent, detect, contain and correct security violations
    a. Risk Analysis (R) – assessment of potential risk and vulnerabilities
    b. Risk Management (R) – identify and implement security measures
    c. Sanction Policy (R) – sanctions against those who fail to comply to security safeguards
    d. Information System Activity Review (R) – Reoccurring and standard review process

2. **Assigned Security Responsibility –** identify security official and role

3. **Workforce Security** – allow access to those permitted to access data and systems and deny access to those not permitted
    a. Authorization and/or Supervision (A) – authorization procedures and documentation
    b. Workforce Clearance Procedures (A) – ensure appropriateness of those with access
    c. Terminating Procedures (A) – when employee terminated/quits, appropriate documentation and processes followed

4. **Information Access Management** – policies and procedures authorizing access
    a. Isolating Health Care Clearinghouse Functions (R) – ensure clearinghouse has appropriate protection policies and procedures
    b. Access Authorization (A) – policy to grant access to workstations, etc.
    c. Access Establishment and Modification (A)– review of authorization and change management when necessary

5. **Security Awareness and Training** – awareness and training programs
    a. Security reminders (A) – meetings, documents, etc. reminding of current policies
    b. Protection from malicious software (A) – policies and procedures guarding against and detecting malicious software
    c. Log-In Monitoring (A) – monitor login events and report/act on discrepencies
    d. Password Management (A) – policy for creating/changing/protecting passwords

6. **Security Incident Procedures –** reporting polices to address security incidents
    a. Response and Reporting (R) – identify, respond and mitigate security incidents

7. **Contingency Plan** – emergency response policies and procedures
    a. Data Backup Plan (R) – retrievable and valid backups
    b. Disaster Recovery Plan (R) – data restoration plan
    c. Emergency Mode Operations (R) – enable ability to maintain plan if working in emergency situation
    d. Testing and Revision Procedures (A) – testing of contingency/emergency plan

e. Application and Data Criticality Analysis (A) – analyze ability to access and safeguard data in contingency/emergency situation

8. **Evaluation** – periodic technical and non-technical evaluation and review of plan

9. **Business Associate Contracts and Other Arrangements** – ensure business partners have approved HIPAA plan
    a. Written Contract or Other Arrangement (R) – get documentation/certification assurance of partners that they are HIPAA compliant

Physical Safeguards

1. **Facility Access Controls –** limit physical access to devices and systems to only authorized personnel
    a. Contingency Operations (A) – establish means to get to lost and restored date due to contingency plan mode
    b. Facility Security Plan (A) – safeguard facility and equipment from unauthorized access
    c. Access Control and Validation Procedures (A) – visitor and support controls
    d. Maintenance Records (A) – Document repairs and modifications to physical components

2. **Workstation Use** – specify functions to be performed on workstations

3. **Workstation Security** – physical safeguards so only authorized users can access workstations

4. **Device and Media Controls –** policies governing handling of items that house HIPAA info
    a. Disposal (R) – ensure security of information on final disposal
    b. Media Re-Use (R)– secure/remove information before reuse on non-secure environment
    c. Accountability (A) – record hardware and media movement
    d. Data Backup and Storage (A) – backup data before movement of equipment

Technical Safeguards

1. **Access Control** – computer and server level access control – people and software
    a. Unique User ID (R)– everyone must have a unique user ID
    b. Emergency Access Procedures (R) – alternate access procedures for accessing information i.e. via the server if workstation fails, etc.
    c. Automatic Logoff (A) – terminate sessions with on predetermined inactivity
    d. Encryption and Decryption (A) – implement or utilize an encryption mechanism

2. **Audit Controls –** audit mechanisms to track changes to EPHI information

3. **Integrity** – ensure no unauthorized alteration or destruction of EPHI

a. Mechanism to Authenticate EPHI (A) – mechanism to corroborate EPHI has not been altered or destroyed thru unauthorized means

4. **Person or Entity Authentication –** verification that entity is who he claims to be
5. **Transmission Security –** prevent unauthorized transmittal of EPHI
    a. Integrity Controls (A) – ensure no improper modification without audit trail
    b. Encryption (A) – encrypt sent and received EPHI – internet, email, FTP, etc.

Organizational Requirements

1. **Business Associate Contracts or Other Assignments** – Ensure business associates comply with corporate policy
    a. Business Associate Contracts (R) – contract to ensure associates, agents and subs adhere to company policies and procedures
    b. Other Arrangements (R) – N/A – only applies in government-to-government contracts
2. **Requirements for Group Health Plans** – N/A – only applicable to group health plan administrators
    a. Implementation Specifics (R) – N/A – see above

Policies and Procedures and Documentation Requirements

1. **Policies and Procedures –** implement appropriate policies and procedures to comply with the standards
2. **Documentation** – maintain policies and procedures in writing
    b. Time Limit (R) – maintain documentation for 6 years
    c. Availability (R) – easily accessible to those who are covered by policies and procedures
    d. Updates (R) – review 'periodically'

Conclusion

Assessing and improving your HIPAA compliance is a daunting task. Even "simplified" guides have numerous policies, procedures and documentation items to maintain. We would suggest breaking your HIPAA effort or assessment into manageable tasks, prioritizing them appropriately, and completing them through regular effort. Your IT support provider will be a valuable partner in assessing and improving the data security required by HIPAA regulations.

Prepared by Surety Technologies Incorporated

"For the life of your company"
www.suretytek.com
info@suretytek.com
402-896-4261
Omaha, Nebraska