

HIPAA SECURITY PRIORITY CHECKLIST

This checklist was developed to guide providers in prioritizing business practices to implement HIPAA's Security standards. Given that resources (i.e., time, money, personnel) may be limited, providers may find it beneficial to review the classifications and apply the checklist items to their own practices. Place a check in the box next to the business practice specified once it is completely implemented. Business practices are classified as either:

CRITICAL – These business practices are critical for compliance with HIPAA's Security standards.

IMPORTANT – These business practices are important for compliance with HIPAA's Security standards.

FUNDAMENTAL – These business practices are fundamental for compliance with HIPAA's Security standards.

SYSTEMS = Healthcare Systems

CRITICAL

Policies and Procedures:

Are your security policy and procedures (including processing violations and user/employee training) in accordance with HIPAA's Security standards?

Designated Security Person:

Do you have a designated person (or system) responsible for:

- Security policy and procedure development and implementation?
- Reporting and processing security violations and questions?
- Reviewing system logs to identify suspect activity and check for security violations, logins, file accesses, etc?
- Scheduling (e.g., daily) and monitoring system logs to evaluate overall security and correct weaknesses?
- Reporting (real or potential/suspected) security violations?
- Monitoring, auditing and supervising technical system maintenance?
- Managing and supervising the conduct of users/employees as it pertains to the physical security of data and facilities?

System Management:

- Do your network security mechanisms (e.g., firewalls, authentication methods, design) ensure the integrity of systems, data, and messages/transactions?
- Is health information encrypted when transmitted outside your internal/private network?

Is access to your systems and networks:

- Controlled so that data cannot be intercepted and interpreted by unauthorized parties
 - both internal and external?
- Restricted to only approved/authorized persons who have a legitimate business need?

Are your systems:

- Security standards documented (and are systems maintained and tested for vulnerabilities based on these standards)?
- Virus prevention mechanisms effective?
- Network tools configured to record access, events and activity, based on HIPAA's Security standards?

Management Process:

Do you have:

- Documented plans to safeguard your building, computer equipment, and electronic information from unauthorized access, tampering, or theft?
- Written and signed Chain of Trust Partner Agreements with all third parties with whom you exchange electronic healthcare data?

User Access Management:

Do user accounts with associated access (i.e., logon, id, password):

- Automatically terminate after a predetermined period (e.g., 15 minutes) of inactivity?
- Uniquely identify the individual user?

Are user accounts with associated access:

- Stored and maintained in a secured manner?
- Protected by the use of biometrics, passwords, pin numbers, telephone callback, or tokens?

IMPORTANT

Policies and Procedures:

Do your security policies and procedures allow for:

- Routine and non-routine receipt, manipulation, storage, dissemination, transmission, and disposal of health information?
- Granting varying levels of access to health care data that includes authorization-level establishment and modification?
- Responding approximately to violations (or suspected violations)?
- User/employee terminations (i.e., removal of user account/access; changing of locks to protected facilities; and turning in keys, tokens, or other access items)?
- Tracking internal and external movement of hardware (e.g., computers, hard drives) and electronic media (e.g., disks, tapes)?
- Recording and escorting facility visitors to areas containing systems?
- How users/employees can use their computers/workstations, including the functions that are to be performed on them?
- Proper and secure physical locations of computers/workstations so that health information cannot be viewed or accessed by unauthorized persons?
- Protecting access to health information where computers/workstations are located in public areas?
- Ensuring that all users/employees with system access are authorized based on pre-established individual or group access roles.

User training:

- Do you provide formal security training for all users/employees with access to systems with periodic reminders, virus protection, login/access monitoring, and password usage/management?

System Management:

Is electronic media:

- Backed up, retrievable, and stored in a secure location?
- Destroyed or disposed of in a manner that protects health information (e.g., reformatting disks, degaussing tapes; scrubbing/scrambling hard drives) before it leaves your control?

Do you have a:

- Reliable mechanism to alarm and/or act on network abnormalities? Are these mechanisms reviewed, enhanced, and tested on an ongoing basis?
- Schedule for logging/recording, auditing, and reporting network events (operational and security) and traffic patterns?
- Documented inventory of all systems?
- Detailed inventory control mechanism to track the movement of hardware and media, including receipts?
- Written contingency plan for responding to emergencies with your operating system (i.e., data backup, disaster recovery) and facilities?
- Disaster recovery (contingency) and emergency operation plan for each facility that is involved in the processing or use of health information?

User Access Management:

- Are access levels maintained and adjusted to reflect job duties, roles, employment status, etc.), and based on the generally accepted “need-to-know” standards?
- Is access to hardware and media adequately monitored and controlled?

FUNDAMENTAL

Policies and Procedures:

- Do your policies and procedures receive periodic management review?

User Training:

- Are records maintained of security training provided to all system users/employees?
- Are users/employees trained in system security? Re-trained when material changes affect their functions?

System Management:

- Are independent internal or external audits performed on systems, applications, and networks on a schedules basis – and/or when significant modifications are made?
- Are detailed records maintained for facility repairs and modifications (e.g., hardware, software, doors, locks, telecommunications equipment)?
- Have you assigned employees or managers to monitor and affect facility safeguards on an ongoing basis?

Piedmont Behavioral Healthcare does not intend this checklist to constitute legal advice. Please direct legal issues and questions to your attorney or HIPAA compliance officer.