

Caregiver System Privacy & Security

Caregiver Alliance Web Services™ is the only consumer-controlled, interoperable personal health record system (PHR) with the security of online banking.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was designed to create uniform standards for transmitting electronic healthcare claims and for protecting the privacy and security of individuals' health-related information. We voluntarily comply with HIPAA privacy and security rules and, as technology evolves and threats to consumers increase, we continuously expand our privacy and security protection processes. Descriptions of some of our HIPAA compliance practices are summarized in the following two tables.

| Table 1. HIPAA Privacy Rule | |
|--|---|
| HIPAA Requirement | Caregiver Compliance Procedure |
| <p>Protected Health Information (PHI). PHI is information, including demographic data, that relates to the individual's: (1) past, present, or future physical or mental health, (2) provision of healthcare; (3) past, present, or future payment for healthcare and that can be used to identify the individual (e.g., name, address, birth date, social security number). The HIPAA Privacy Rule applies to all PHI.</p> | <p>All information in a Caregiver client account is treated as PHI even if the information is not health related or not useful in identifying the individual. No one may access the account without explicit client authorization and system authentication.</p> |
| <p>Personal Representative (PR). A covered entity is required to treat a PR the same as the individual with respect to uses and disclosures of the individual's PHI as well as the individual's rights under the privacy rule. In most cases, parents are the PRs for their minor children.</p> | <p>Client accounts are managed by the consumer or designated account administrator (personal representative). The account administrator may be a parent, guardian, or adult child of a disabled parent or a care coordinator employed by the consumer or by a service agency. For brevity, we assume below that all consumers are their own account administrators.</p> |
| <p>Covered Entity (CE). HIPAA applies to health plans, healthcare clearinghouses, and to any healthcare provider who transmits health information in electronic form.</p> | <p>Consumers may grant user privileges on client accounts to healthcare providers, to individuals who represent their health insurance plans, and to representatives of healthcare clearinghouses. Health insurance and healthcare clearinghouse representatives may be authorized for read-only access to insurance information.</p> |
| <p>Business Associate (BA). A BA is a person</p> | <p>The consumer chooses which individuals</p> |

Caregiver System Privacy & Security

| Table 1. HIPAA Privacy Rule | |
|---|---|
| HIPAA Requirement | Caregiver Compliance Procedure |
| <p>or organization that performs functions on behalf of a covered entity (CE) without being employed by the entity. HIPAA requires that the CE have a contract with the BA that includes certain protections for individuals' health information.</p> | <p>should have user privileges on a Caregiver client account. Each consumer-authorized user has a unique, user-ID for entry into each client account with specific, client-conferred audited privileges. All users are authenticated by the system as a condition of system access. The doctor or BA directly requests account privileges from the consumer.</p> |
| <p>Disclosure. A covered entity may not use or disclose PHI except: (1) as the privacy rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.</p> | <p>A consumer must explicitly authorize user access to the client account in order for an individual to use or disclose account information. If a consumer-authorized user is covered by HIPAA, that user may choose to disclose account information "as the privacy rule permits or requires." It is the sole responsibility of that user to comply with provisions of the privacy rule.</p> |
| <p>Consent to use or disclose PHI. Written permission from individuals to use and disclose their PHI for treatment, payment, and healthcare operations is optional for all covered entities.</p> | <p>When a consumer authorizes a user for privileges on the account, the consumer sends an electronic message to the new user that indicates willingness to sign the HIPAA-covered user's specific consent form.</p> |
| <p>Incidental use and disclosure. The privacy rule does not require that every risk of an incidental use or disclosure of PHI be eliminated as long as the covered entity has adopted reasonable safeguards and the information being shared was limited to the minimum necessary.</p> | <p>Consumers may minimize the risk of incidental use or disclosure of PHI by asking their doctors to identify employees and business associates who need to be authorized with client account privileges and unique user-IDs. The client account audit trail documents each user's actions in the account and safeguards both the consumer and the doctor.</p> |
| <p>Authorization. A covered entity must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment, or healthcare operations, or otherwise permitted or required by the privacy rule.</p> | <p>Covered entities, and all other authorized users on client accounts, exchange secure Web messages (behind firewalls) with account administrators to obtain necessary authorizations.</p> |

Caregiver System Privacy & Security

| Table 1. HIPAA Privacy Rule | |
|---|---|
| HIPAA Requirement | Caregiver Compliance Procedure |
| <p>Psychotherapy notes (PN). A CE must obtain an individual's authorization to use or disclose PN except: (1) CE who originated notes may use PN for treatment, (2) CE may use or disclose PN for training, legal defense, HHS investigation of compliance with privacy rule, public safety, and as law requires.</p> | <p>A HIPAA covered user, authorized on many client accounts, may employ a Caregiver enterprise account to store psychotherapy notes.</p> |
| <p>Minimum necessary standard (MNS). A CE must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request. When the MNS applies, a CE may not use, disclose, or request the entire medical record unless it can specifically justify this action.</p> | <p>Consumers may insure minimum necessary disclosure by authorizing client-account users for specific privileges on specific client account components. If users want to disclose more information they must seek authorization for additional privileges from the account administrator.</p> |
| <p>Role-based access. A CE must implement policies and procedures that restrict access to PHI based on specific roles of workforce members. They must identify classes of persons who need access to PHI, the categories of PHI to which access is needed, and conditions under which they need PHI to do their jobs.</p> | <p>The security and privacy officer of a CE may employ a Caregiver enterprise account to: (1) assign potential client account roles to workers consistent with their job descriptions and (2) request role-based authorization from client account administrators.</p> |
| <p>Right to review (RR). Individuals have the right to review and obtain a copy of their PHI in a CE's designated record set (DRS). The DRS is that group of records maintained by or for a CE that is a provider's medical and billing records, health plan's enrollment, payment, claims adjudication, and case or medical management record systems.</p> | <p>A HIPAA covered, client-authorized user may update the client account so as to give consumers a continuous RR. Or, consumers may exercise their RR, obtain copies of all their healthcare records, and store them in the client account.</p> |
| <p>Amendment. Individuals have the right to have CEs amend their PHI when information is inaccurate or incomplete. If a CE accepts request, it must make reasonable efforts to provide amendment to persons that the individual has identified as</p> | <p>A consumer may insure that inaccurate or incomplete information is amended and accessible to people who need it. The consumer makes an entry in a relevant everyday chart (e.g., mental health), notes the corrections in the entry, uploads and</p> |

Caregiver System Privacy & Security

| Table 1. HIPAA Privacy Rule | |
|---|--|
| HIPAA Requirement | Caregiver Compliance Procedure |
| needing it. If the request is denied, CEs must include individual's statement of disagreement in record. | links the inaccurate document to the entry, and notifies authorized users about the amendment. |
| Disclosure accounting. Individuals have a right to an accounting of the disclosure of their PHI by a CE or by the CE's business associates. The maximum disclosure accounting period is 6 years immediately preceding the request and following the CE's privacy rule compliance date. | The security and privacy officer of a CE may employ the audit trail of a Caregiver enterprise account to supply disclosure accounting to a consumer. And, the client account administrator may employ the client account audit trail for continuous disclosure accounting. |
| Confidential communication. Health plans and covered healthcare providers must permit individuals to request an alternative means for receiving PHI by means other than that the CE typically employs. CEs must accommodate reasonable requests and may not question the individual's statement of endangerment. | A consumer may request that a CE transmit PHI by exercising client-conferred privileges in the client account. |

Caregiver System Privacy & Security

| Table 2. HIPAA Security Rule | |
|--|---|
| HIPAA Requirement | Caregiver Compliance Procedure |
| Risk analysis. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information. | Conducts comprehensive and ongoing risk analysis consulting leading experts in the field. |
| Risk management. Implement security measures sufficient to reduce risks and vulnerabilities. | Implements a comprehensive and dynamic security policy, consistent with the HIPAA Security Rule. |
| Sanction policy. Apply appropriate sanctions against workforce members who fail to comply with security policies and procedures. | Immediately terminates relationship with any workforce member or business partner failing to comply with security policy and takes appropriate legal action. |
| Information system activity review. Implement procedures to regularly review records of information system activity. | Continuously reviews system logs and responds to automated emergency alerts. |
| Authorization and/or supervision. Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information. | Allows access to electronic protected health information database by System Administrator and supervised designees. |
| Workforce clearance procedure. Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | Workforce members screened for suitability before access to electronic protected health information database is allowed. |
| Termination procedures. Implement procedures for terminating access to electronic protected health information when the employment of a workforce member. | In the event a Caregiver Alliance Applications workforce member is terminated, passwords and access keys are changed immediately and prior to informing employee in order to avoid possible malicious activity. |
| Isolating healthcare clearinghouse functions. If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | Prosocial Applications is not part of a larger organization. |
| Access authorization. Implement | Access to electronic protected health information |

Caregiver System Privacy & Security

| Table 2. HIPAA Security Rule | |
|--|---|
| HIPAA Requirement | Caregiver Compliance Procedure |
| <p>policies and procedures for granting access to electronic protected health information.</p> | <p>database is controlled and monitored by System Administrator.</p> |
| <p>Access establishment and modification. Implement policies and procedures that establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.</p> | <p>Oversees modification of access privileges to electronic protected health information database.</p> |
| <p>Security reminders. Periodic security updates.</p> | <p>Periodic security reviews are conducted and training is implemented if necessary.</p> |
| <p>Protection from malicious software. Procedures for guarding against, detecting, and reporting malicious software.</p> | <p>Server hosting facility monitors network for suspicious activity and network intrusions, and automatically reports and logs security events.</p> |
| <p>Log-in monitoring. Procedures for monitoring log-in attempts and reporting discrepancies.</p> | <p>Checks daily logs for suspicious activity.</p> |
| <p>Password management. Procedures for creating, changing, and safeguarding passwords.</p> | <p>Passphrase allowing access to electronic protected health information database is known only to System Administrator, and is kept under lock and key in the event the System Administrator is unavailable.</p> |
| <p>Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents; and document security incidents and their outcomes.</p> | <p>Comprehensive records of any and all suspected or confirmed security incidents are documented and reported. System Administrator undertakes methods of mitigating harmful effects, and modifies security procedures accordingly.</p> |
| <p>Data backup plan. Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.</p> | <p>Secure database replication ensures records will be available from a separate server if primary server is incapacitated.</p> |
| <p>Disaster recovery plan. Establish (and implement as needed) procedures to restore any loss of data.</p> | <p>Secure database replication ensures records will be available from a separate server if primary server is incapacitated.</p> |
| <p>Emergency mode operation plan. Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.</p> | <p>Secure database replication ensures records will be available from a separate server if primary server is incapacitated.</p> |

Caregiver System Privacy & Security

| Table 2. HIPAA Security Rule | |
|--|---|
| HIPAA Requirement | Caregiver Compliance Procedure |
| Testing and revision procedures. Implement procedures for periodic testing and revision of contingency plans. | Performs ongoing health and availability and regular penetration testing to insure system is stable and secure. |
| Applications and data criticality analysis. Assess the relative criticality of specific applications and data in support of other contingency plan components. | One application (Caregiver) is the only application, and contains all of critical data and supports the Caregiver. |
| Written contract or other arrangement. Document the satisfactory assurances required by the HIPAA security rule through a written contract with third party business associates. | Agreements are obtained from all third party business associates who may have access to HIPAA-covered information |
| Contingency operations. Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | Secure database replication ensures records will be available from a separate server if primary server is incapacitated. |
| Facility security plan. Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. | Access to hosting facility is strictly limited to company-authorized technical staff and escorted visitors. Access to the datacenter and attached facilities requires a card-key. Electronic security systems controlled datacenter access and are accompanied by a full complement of motion detectors that are strategically placed throughout the entire facility. The security system is fully logged and monitored locally and remotely. |
| Access control and validation procedures. Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. | System Administrator controls, grants and oversees access to hosting facilities by designees |
| Maintenance records. Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security. | Hosting facility maintains maintenance records of repairs and modifications to physical components of secure facility. System Administrator maintains hardware maintenance and modification records. |
| Workstation use. Implement policies | Access to electronic protected health information |

Caregiver System Privacy & Security

| Table 2. HIPAA Security Rule | |
|---|--|
| HIPAA Requirement | Caregiver Compliance Procedure |
| and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | database is based on login ID and passwords, and system authentication, and is not related to specific workstations. |
| Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. | Access to EPHI is based on login ID and passwords, and system authentication, and is not related to specific workstations. |
| Disposal. Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. | A firm specializing in data removal will erase any original physical media, and the firm will certify removal of data. |
| Media re-use. Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use. | A firm specializing in data removal will erase the original physical media, and the firm will certify removal of data. |
| Accountability. Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | System Administrator is responsible for maintaining these records. |
| Data backup and storage. Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. | Secure database replication ensures records will be available from a separate server if primary server is incapacitated. |
| Unique user identification. Assign a unique name and/ or number for identifying and tracking user identity. | Users log into the server with unique IDs and passwords and are authenticated by the system prior to system access. |

Caregiver System Privacy & Security

| Table 2. HIPAA Security Rule | |
|---|--|
| HIPAA Requirement | Caregiver Compliance Procedure |
| <p>Emergency access procedure. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.</p> | Secure database replication ensures records will be available from a separate server if primary server is incapacitated. |
| <p>Automatic logoff. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.</p> | Users logged on and inactive for more than 30 minutes are automatically logged out of the system. |
| <p>Encryption and decryption. Implement a mechanism to encrypt and decrypt electronic protected health information.</p> | Data are fully encrypted during transmission with SSL (https protocol). Database file system is encrypted. |
| <p>Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.</p> | Caregiver accounts contains an audit table that records logins, document access, and security violations. Alerts regarding violations are automatically sent to System Administrator. |
| <p>Mechanism to authenticate electronic protected health information. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.</p> | All data on the system are accessible only through Caregiver code. Once entered, electronic personal health data are permanent and unalterable. |
| <p>Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.</p> | Authorized users receive unique user IDs and passwords and are cautioned against sharing of same. Users may be penalized or excluded from system use for password sharing. |
| <p>Integrity controls. Implement security measures to ensure that electronically transmitted electronic protected health information are not improperly modified without detection until disposed of.</p> | Once entered, electronic protected health information data are permanent and unalterable. |
| <p>Encryption. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.</p> | Servers use SSL encryption ensures encryption between users and servers and vice versa. Encryption key for SSL certificate is accessible by passphrase known only to System Administrator. Web server is neither directly or indirectly accessible without passphrase. |