



SECURITY, PRIVACY AND HIPAA POLICIES

SPRINGCM | Committed to Serving the Healthcare Industry

SPRINGCM

SECURITY, PRIVACY AND HIPAA POLICIES

SpringCM extends its commitment to protecting and securing personal data by following the general philosophy found in applicable security regimes, including the Health Insurance and Portability and Accountability Act and its implementing regulations (collectively "HIPAA"), such as adopting appropriate physical, technical and administrative safeguards to protect client confidential and personal information, including data which HIPAA defines as Protected Health Information (PHI). The following applies to SpringCM functionality and safeguards, which will apply to our customers' data:

A. HIPAA

The greatest burdens that HIPAA places on covered entities include:

- I. HIPAA's Individual Rights Provisions: Allowing an individual access their record on demand and allowing an individual to see a record of when and to whom the record has been disclosed
- II. HIPAA's Security Rule: Adequately securing Protected Health Information (PHI)
- III. HIPAA's Document Retention Policy: Six year mandatory document retention
- IV. HIPAA's Audit Trail Policy: Ensuring identification of who accesses documents and when, where and how

Here's how SpringCM can help you manage your HIPAA compliance obligations:

Compliance

The documents managed through our system can help a covered entity, or business associate of a covered entity, timely respond to individual requests for access, amendment and disclosure accounting. SpringCM's secure document repository, and powerful search capabilities, allow organizations the ability to electronically store, locate and manage large volumes of documents in a fraction of the time compared to traditional filing processes.

For example:

- SpringCM enables a covered entity to easily search its entire database and quickly assemble an individual's entire history of PHI to respond to an access request.
- SpringCM helps track disclosures of PHI as certain settings can be modified to track a disclosure to another entity. Along those lines, SpringCM can be used to capture certain data required for an accounting (through keywords) such as a list of persons to whom the document is disclosed, a brief description of the disclosure, the date, etc.
- A new document can easily be created, stored and tagged for later retrieval to satisfy amendment requirements when the covered entity agrees to make an amendment to PHI on behalf of the individual.

Security Rule Compliance

HIPAA requires covered entities to implement reasonable technical, administrative and physical safeguards to ensure the confidentiality of PHI. Those safeguards should be appropriate for the size and complexity of the covered entity's business. To that end, SpringCM provide a sophisticated and comprehensive security model.

Our technical controls include:

- Technical safeguards to secure client's personal information where data is hosted. These safeguards include: firewalls, Intrusion Prevention Systems, Secure Socket Layer (SSL) encryption over the public Internet for web-facing applications, authentication for remote access and comprehensive protection against malware (malicious software) at Internet gateways, email gateways, file servers and desktops. SpringCM hardens its servers (i.e., permanently shuts down certain services if not in use) and engages in diligent security patch management to remediate vulnerabilities on servers.
- Clients may also audit the SpringCM security programs on an annual basis, subject to applicable client confidentiality and security policies.

Our administrative controls include:

- Role-based access control policy to restrict access to all computerized information through a strong password system.
- Access to software or data is prohibited unless specifically authorized by use of such password and granting of rights by the administrator of the client's account
- Users are only given access to the system resources that contain personal data to the extent necessary to perform their roles. All other access to computer resources requires the approval of the data owner, who is typically a business leader responsible for the business functions supported by that data owner.
- Clients should give careful consideration to access granted only to specific areas related to that user's job function authorize those functions through the covered entity's Information Security Officer.

Our physical controls include:

- To protect PHI, SpringCM locates all enterprise data on SpringCM's state of the art hosting environment located with Qwest Communications, a tier one hosting provider.
- SpringCM regularly performs third-party security audits.
- Among other features, your data is housed on a fully redundant, highly available, Storage Access Network (SAN) in a restricted access area; access is restricted to by badge reader systems, biometrics access control (hand-readers) and a facility guard staff.
- Only SpringCM's key employees are given access to our system storage at Qwest Communications.
- SpringCM routinely reviews Qwest's SAS 70s for our vendor and performs on-site monitoring.

Document Retention and HIPAA Compliance Audits

HIPAA requires covered entities to retain copies of certain documents for six years. The SpringCM system offers virtually unlimited storage capacity. Because of our document creation profiles, a client can indicate whether a particular document should be stored or deleted after a certain period of time. Again, advanced search capabilities help locate documents in the case that the covered entity was subject to an investigation by the Secretary of Health and Human Services for HIPAA compliance or subject to another type of court process, such as a subpoena.

B. SpringCM Commitment to Privacy and Security

SpringCM not only designs functionality that supports privacy and security, but also the company operates in a manner that underscores its importance.

For example:

Information Security and Privacy Policies

- SpringCM has adopted an Information Security Policy and a Privacy Policy that establishes uniform security and privacy standards for SpringCM operations.
- SpringCM has based its Information Security Policy on BS7799/ISO, an internationally recognized information security management standard.

Administrative Officers

- SpringCM has a dedicated centralized information security organization led by its Chief Technology Officer (CTO). The CTO reports directly to SpringCM's Chief Executive Officer (CEO).

Privacy Training

- SpringCM conducts privacy and security education across the firm that augments training regarding the confidentiality and security of personal information.

Confidentiality Agreements

- All SpringCM associates execute a comprehensive confidentiality agreement as a condition of their employment by SpringCM. These agreements impose obligations on SpringCM associates to protect the confidentiality and security of client confidential and personal information, including PHI.

Business Associate Agreements and Controller-Processor Agreements to Contractually Protect Transfers of Personal Data

- SpringCM is not a covered entity. However, because our business interfaces with and supports different types of covered entities, such as health plans, providers and clearinghouses, we will enter into mutually agreeable business associate agreements (or sub-business associate agreements) when requested by clients. Upon request, we can provide a sample of our standard business associate agreement.
- To the extent that SpringCM subcontracts processing activities to third parties, it requires such third parties to execute agreements that establish adequate safeguards around the collection, storage, processing and disposal of client confidential and personal information.

If you have any additional questions on SpringCM's HIPAA, security or privacy policies please contact sales@springcm.com or call 877.362.7273