SmartVault® — HIPAA Compliance

About HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law requiring health care organizations to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of patient information.

What you don't know *can* hurt you

Under HIPAA, penalties for non-compliance can include fines of up to $50,000 per violation, with fines for officers and directors of up to $250,000 per violation. The provisions include criminal penalties of up to 10 years in prison.[1]

I'm not a health care organization. Does HIPAA apply to my business?

Under HIPAA, covered entities include health plans, health care clearinghouses, and health care providers regardless of size who electronically store or transmit any health information in connection with any transactions for which HHS (Department of Health and Human Services) has adopted a standard.[2]

In addition to covered entities, HIPAA includes a class of individuals and businesses called Business Associates. A business associate is defined as any business, regardless of size that performs function or activities on behalf of a covered entity, including creating, receiving, maintaining, or transmitting protected health information on behalf of another business associate.

(i) How does SmartVault support you in complying with HIPAA?

HIPAA Requires	SmartVault Responds
Business Associate Agreements	As a provider of services to health care organizations, SmartVault makes available a standardized Business Associate Agreement (BAA) to govern our storage and protection of your client records. This agreement can be obtained from your sales representative for execution by your management/legal team and the compliance officer of SmartVault.
Comprehensive written Information Security Program	**SmartVault's information security program is clearly documented**, with supporting policies and procedures for all aspects of safeguarding your information, and it is reviewed on an annual basis to ensure it is still meeting the needs of the changing business landscape.
Risk Assessment and Remediation	On an annual basis, we at SmartVault evaluate not only our own internal processes and controls, but also those of our data center providers.
Administrative Safeguards	As part of the administrative safeguards in place at SmartVault, each and every employee has clearly defined roles and responsibilities for protecting our customer's data. We provide training on information security to all new hires, and on an annual basis to all employees and contractors. We also have clearly documented processes and procedures for every aspect of our services and ensure that our staff understand and operate by those procedures.

---

[1] HIPAA Violations and Enforcement
[2] To Whom Does the Privacy Rule Apply and Whom Will It Affect?

(i) How does SmartVault support you in complying with HIPAA? *continued*

HIPAA Requires	SmartVault Responds
Technical Safeguards	**Industry Standard SSL encryption for documents in transit** – protecting your documents, passwords and interactions with SmartVault from eavesdropping **Granular access** – ability to grant access to specific folders **Activity Logs** – complete audit history of who accessed and/or modified documents stored in SmartVault **Document access via authenticated login** – files are only accessible to users of the service (no anonymous sharing of files)
Physical Safeguards	**Physical access to our data centers is strictly controlled**. Only those employees and contractors with a demonstrated need are permitted access and that access is controlled through a series of technical controls such as badge readers on the doors, biometric locks on the data center and physically keyed or combination locks on cabinets and safes.
An ongoing process to determine whether the Security Program is effective	**At SmartVault, we are constantly seeking to improve our services and security is no exception**. We continuously gather and analyze new information regarding threats and vulnerabilities, adjusting our security controls to ensure their effectiveness in the face of these changes. And we update our security strategy, the administrative, technical and physical safeguards to ensure we are providing our customers with the most comprehensive protection that we can.

In summary

Keep in mind that HIPAA compliance is a health care organization obligation, not a prescriptive specification. So when we say that SmartVault supports a HIPAA compliant workflow, what we mean is that our service gives you the tools that health care organizations and service providers need in order to work in a HIPAA-compliant fashion.

While we are not a HIPAA compliance consulting firm, we are happy to assist you in getting pointed in the right direction. Feel free to contact us at **security@smartvault.com** for more insight.

About SmartVault

SmartVault adds value to your securities workflow by giving you the ability to store all of your files securely online, access documents when you need them, and safely share files with the right people. It's easy for you to use with features specifically designed for banking and securities companies to automate workflow and meet compliance mandates.