

My Docs Online HIPAA Compliance

Updated 2/1/2010

Using My Docs Online in a HIPAA-compliant fashion depends on following proper usage guidelines, which can vary based on a particular use, but have several general characteristics.

For instance, medical transcriptionists and similar services ("Business Associates"), as well as physicians and other providers ("Covered Entities") should:

- Use the Transcription or Enterprise Edition.
- Assign individual subaccount IDs to each "covered entity" and to each MT.
- Avoid the shared use of individual subaccount IDs.
- Enforce transmission encryption by requiring the use of SSL for all subaccounts.
- Set appropriate folder permissions based on the access privileges of each subaccount.
- Safeguard login IDs and passwords.
- Avoid the inclusion of individually identifiable information in the names of uploaded files or comments associated with files.

HIPAA Rules and Regulations As They Apply to My Docs Online

Important definitions:

HIPAA *The Health Insurance Portability and Accountability Act of 1996*

HIPAA established and continues to govern Privacy and Security Rules for the handling of medical information, by "Covered Entities" and their "Business Associates". Covered Entities include health care providers (doctors, hospitals, etc.) and health plans. Business Associates include companies and consultants that perform services for "covered entities". Medical Transcription services are an example of a Business Associate, and these MT services are often My Docs Online customers, which makes My Docs Online a business associate by extension. In other cases a Covered Entity is a My Docs Online customer, which makes us the Covered Entity's Business Associate. In these cases it is common for a Business Associate Agreement to be in place between the Covered Entity and My Docs Online.

ARRA: *American Recovery and Reinvestment Act of 2009 (commonly known as the "Stimulus Package")*

The most significant change brought about by ARRA as it relates to HIPAA and My Docs Online is that, beginning in 2010, as a Business Associate, MDO is directly subject to HIPAA under the ARRA and is governed by the same requirements under HIPAA as covered entities. Business Associates such as MDO were previously subject to security and privacy requirements through their contracts with covered entities.

HITECH: *The Health Information Technology for Economic and Clinical Health Act*

Requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information.

The HIPAA Privacy Rule

Provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

The HIPAA Security Rule

Specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information. Maintaining proper security is the main goal of My Docs Online's HIPAA Policies and the My Docs Online Security Policies and Procedures Plan.

Security Breach Notification Requirements

ARRA established more stringent security breach notification requirements and gives increased notification to patients. Under the ARRA, covered entities and business associates must provide notification to any person whose protected health information has been breached. The ARRA also provides requirements for such notifications.

HIPAA Security Rule Goals and Objectives and How My Docs Online Complies

As required by the "Security standards: General rules" section of the HIPAA Security Rule, each covered entity (and beginning in 2010, each Business Associate) must:

- Ensure the confidentiality, integrity, and availability of EPHI (Electronic Protected Health Information) that it creates, receives, maintains, or transmits
- Protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule

Security Rule Standard Components

Administrative Safeguards

Defined in the Security Rule as the "administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

Physical Safeguards

Defined as the "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

Technical Safeguards

Defined as the "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

Organizational Requirements

Includes standards for business associate contracts and other arrangements, including memoranda of understanding between a covered entity and a business associate when both entities are government organizations; and requirements for group health plans.

Policies and Procedures and Documentation Requirements

Requires implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of the Security Rule; maintenance of written (which may be electronic) documentation and/or records that includes

policies, procedures, actions, activities, or assessments required by the Security Rule; and retention, availability, and update requirements related to the documentation.

These security rule components, safeguards, and requirements are met by the policies and procedures documented in the My Docs Online Security Policies and Procedures Plan, which can be made available to our customers as needed.

Breach Notification

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

There are three exceptions to the definition of "breach"

- The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate.
- The second exceptions applies to the inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
- The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

If a breach has occurred, covered entities and business associates must demonstrate that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. Covered entities must have in place written policies and procedures regarding breach notification. The My Docs Online policies and procedures for handling breach notification are contained in the My Docs Online Security Policies and Procedures Plan, which can be made available to our customers as needed.