

What is HIPAA?

HIPAA stands for the Health Insurance Portability & Accountability Act of 1996, Public Law 104-191, which amends the Internal Revenue Service Code of 1986. It is also known as the Kennedy-Kassebaum Act. HIPAA calls for:

- Standardizing electronic patient health, administrative and financial data
- Establishing unique health identifiers for individuals, employers, health plans and health care providers
- Implementing security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present, or future

What Must You Do?

HIPAA requires all organizations to protect information as set forth in the Privacy Rule. The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information" (PHI). This protection extends to maintaining sufficient safeguards and infrastructure to "ensure the confidentiality, integrity, and availability of all electronic protected health information."

Second, HIPAA specifies that an individual has a right to receive an accounting of disclosures of PHI made by a covered entity in the six years prior to the date on which the accounting is requested. This means healthcare organization must retain all records and documents that contain PHI for at least six years in the event an audit request is received.



Who Does HIPAA Effect?

Any organization that electronically stores or transmits individually "identifiable healthcare information" must comply with HIPAA regulations. If your organization is a healthcare provider, healthcare plan, payer, transaction clearinghouse, billing agency or other entity that processes healthcare data you are subject to HIPAA regulations. Even a single-physician office must comply with HIPAA rules.

Why Must You Do It?

HIPAA calls for severe civil and criminal penalties for noncompliance, including fines up to \$25,000 for multiple violations of the same standard in a calendar year and fines up to \$250,000 and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information.

What Does Iomega Provide?

Iomega's Data Continuity Solutions provide a foundation to protect the confidentiality and security of "individually identifiable health information" so to comply with the law and avoid any civil and criminal penalties. Deploying an Iomega data continuity solution to backup data, your practice begins to meet the "availability, integrity and technical safeguards" security standards for the protection of electronic "protected health information."

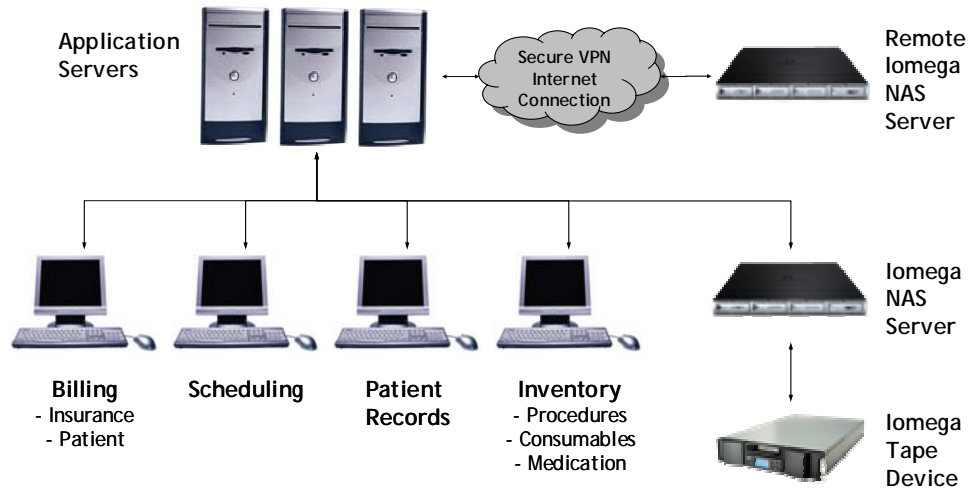
If you answer "YES" to any of the following questions, one of the Iomega solutions described on the reverse will help you to meet your needs:

- Do you electronically store or transmit "individually identifiable healthcare information"?
- Are you concerned about complying with HIPAA to "ensure the confidentiality, integrity, and availability of all electronic protected health information"?
- Are you interested in solutions that comply with HIPAA regulations for managing "protected healthcare information" for the six years as required by law?

HIPAA COMPLIANCE SOLUTION

iomega's NAS Servers provide a foundation for protecting "individually identifiable health information" for your healthcare organization's processes to comply with the law and avoids any civil and criminal penalties.

Deploying an iomega data continuity solution to backup your information, your healthcare organization has a technical platform to comply with the "availability, integrity and technical safeguards" security standards to manage electronic "protected health information." The diagram illustrates a potential HIPAA compliance foundation.



Protection Level	Description
Level 1 "Basic"	Installing an iomega NAS server is an easy & cost-effective way to store electronic patient information. Regularly backing up files to an iomega NAS server ensures the information remains safe in case of inadvertent deletions, server failures, operator error or other disasters.
Level 2 "Enhanced"	Adding an iomega Tape Device or iomega REV™ 35GB/90GB Drive to an iomega NAS server achieves an additional level of protection by providing a backup to the NAS server. This step allows you to archive historical patient information and records to tape for off site storage in the event of a site disaster.
Level 3 "Maximum"	Adding a second iomega NAS server in a remote location and connecting it to your office network through a secure virtual private network (VPN) allows you to maintain an exact copy of your practice information at all times. In the event of a disaster at either location, one copy of your information is always accessible.

Protection Level	Practice Size				
	1-4 Employees	5-9 Employees	10-19 Employees	20-49 Employees	50+ Employees
Level 1 "Basic"	iomega NAS 300m 240GB	iomega NAS 400m 320GB	iomega NAS 400m 640GB	iomega NAS 400m 1TB	iomega NAS 400m 1TB
Level 2 "Enhanced"	iomega NAS 300m 240GB plus iomega REV 35GB/90GB Drive	iomega BACKUP 320m	iomega BACKUP 640m	iomega BACKUP 640m	iomega BACKUP 640m
Level 3 "Maximum"	2x iomega NAS 300m 240GB plus iomega REV 35GB/90GB Drive	iomega NAS 400m 320GB plus iomega BACKUP 320m	iomega NAS 400m 640GB plus iomega BACKUP 640m	iomega NAS 400m 640GB plus iomega BACKUP 640m	iomega NAS 400m 1TB plus iomega BACKUP 640m

S I M P L E S T O R A G E F O R A C O M P L I C A T E D W O R L D . ™