

Is your security at risk?



HIPAA

HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT

MAYLINE® GROUP

Any time a patient visits with a doctor, is admitted to a hospital, receives a prescription, or sends in a claim to a health insurance company, a record is made of the health information. Currently, many medical field and other health care providers store medical records in an open shelf environment, which allows information to be visible and exposed. Today, the use and disclosure of this information is protected by a variety of state laws, leaving huge holes in the protection of patients' privacy and confidentiality rights.

What is HIPAA

HIPAA is the acronym for the Health Insurance Portability and Accountability Act of 1996. HIPAA is the largest government action in Healthcare since Medicare. In recognizing the need for a national patient record privacy standard, the federal government established this act with the primary purpose of improving health insurance accessibility for people changing employers or leaving the workforce. This federal legislation also provides provisions to encourage and protect health-related data, ensure privacy, and improve efficiency throughout the health care system. HIPAA consists of two standards: the security standard and privacy standard.

"The **SECURITY STANDARD** relates to the technical and physical protection of protected health information, which includes computer passwords, network firewalls, locked file cabinets and file rooms that contain patient records."—*Massachusetts Medical Society Online Directory*

WHAT IS THE INTENT OF THE SECURITY STANDARD?

- To secure all medical records and other individually identifiable health information used or disclosed, in any form (i.e. paper, oral or electronic communication).
- To improve patients' rights over both understanding and controlling how their health information is used.
- To require health care providers to give patients clear written explanations of how health information may be used.
- To allow patients to see and receive copies of all their records as well as a history of non-routine disclosures.
- To require patient consent before information is released.

"The **PRIVACY STANDARD** relates to the policies and procedures protecting patients' health information, such as consent and authorization forms, privacy notices and business associated agreements."

—*Massachusetts Medical Society Online Directory*

WHAT IS THE INTENT OF THE PRIVACY STANDARD?

- To provide information to patients about their privacy rights.
- To adopt written privacy procedures for staff and employees.
- To train employees on privacy procedures and designate a "privacy" officer within the organization.
- To secure patient records containing individual health information so they are not readily available to those who do not need them.



WHAT ARE THE KEY ELEMENTS OF HIPAA?

- Security standards to protect and secure electronic, paper and oral communications.
- Privacy regulations to protect individuals privacy rights in regards to health information.
- National standards for electronic transmissions of health care data.
- Standardization on establishing patient "identifiers" for employers and health care providers.

WHO MUST COMPLY WITH HIPAA?

Almost everyone. As required by HIPAA, the final regulation covers health plans, health care clearinghouses, health care providers, physician offices, employers, public health authorities, life insurers, information systems vendors, service organizations, and universities. All who conduct certain financial and administrative transactions through paper, oral or electric communications.

WHEN IS THE HIPAA COMPLIANCE DEADLINE?

April 14, 2003! The Final Rule published in August 2002 requires that all physicians, health care providers, clinics, hospitals, health claim processors and any other parties providing treatment or claims processing to comply with privacy regulations by April 14th 2003.

WHO WILL BE ENFORCING THE HIPAA REGULATIONS?

The Department of Health and Human Services (DHHS). The DHHS will publish a final draft in early 2003 concerning the enforcement of HIPAA regulations. This publication will address the compliance provision and detail how it will be enforced and how penalties will be imposed.

WHAT ARE THE RAMIFICATIONS FOR NON-COMPLIANCE?

Civil and Criminal penalties may be imposed for noncompliance. In addition, there may be fines that will not exceed \$100 per violation per person or entity. The total amount imposed on any one person for a violation of any one requirement, could reach \$25,000 in a calendar year.

Criminal penalties and fines may be imposed if protected health information is used or disclosed with illegal intent.



**THE PRICE FOR
NON-COMPLIANCE:
XFINES
XPENALTIES**

WHAT DOES THE MAYLINE GROUP OFFER TO COMPLY WITH HIPAA?



ARC Rotary File

Increases filing capacity while providing a locked and secure storage environment for patient files and records, as well as mixed media.

4-Post Shelving on an 810 Manual or 820 Mechanical Assist Mobile System: Stores large quantities of files to maintain space efficiency and work productivity while offering a compacting design with floor lock security.



Mobile Aisle

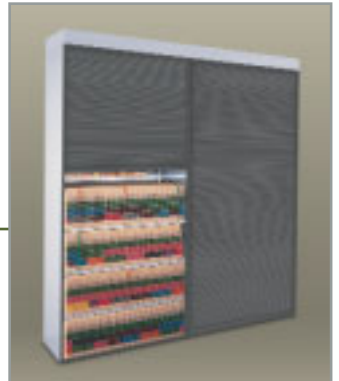


File Harbor

A multi-media cabinet with horizontal-receding tambour doors and security lock.

File Harbor on Kwik-Track: Multi-media, locked cabinet mobilized in a two or three row configuration combining both security and space efficiency.

Security Shade: An easily installed vertical locking tambour door designed to provide security and privacy to 4-Post Shelving.



Security Shade



Flip-N-File

Flip-N-File Cabinet: Independent retractable flipper door cabinet with gang lock available in 5, 6 and 7 tier heights.

Data/LAN Cabinets: Designed to provide a secure environment with a variety of locking options for computer equipment and electronic files. All cabinets are ventilated and equipped with efficient cable management.



Data/Lan Cabinets

