April 14, 2003 -- *Under the security standards announced today, health insurers, certain health care providers and health care clearinghouses must establish procedures and mechanisms to protect the confidentiality, integrity and availability of electronic health information. The rule requires covered entities to implement administrative, physical and technical safeguards to protect electronic health information in their care.*[1]

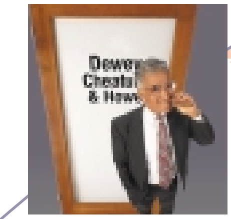
www.newera.com

Do You Know if You are in Compliance?

What Your IT Audit Staff Should Know about HIPAA

HIPAA – Health Insurance Portability and Accountability Act

The first-ever federal privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers took effect on April 14, 2003. Developed by the Department of Health and Human Services (HHS), these new standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country. Congress called on HHS to issue patient privacy protections as part of the Health Insurance Portability and Accountability Act (HIPAA). HIPAA included provisions designed to encourage electronic transactions and also required new safeguards to protect the security and confidentiality of health information. The final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., enrollment, billing and eligibility verification) electronically. Most health insurers, pharmacies, doctors and other health care providers were required to comply with these federal standards beginning April 14, 2003. As provided by Congress, certain small health plans have an additional year to comply.[2]



According to the National Research Council, individually identifiable health information frequently is shared with consulting physicians, managed care organizations, health insurance companies, life insurance companies, self-insured employers, pharmacies, pharmacy benefit managers, clinical laboratories, accrediting organizations, state and federal statistical agencies, and medical information bureaus.[3]

Risk analysis is a key requirement of the HIPAA final Security Rule. The Security Rule requires covered entities (CEs) to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronically protected health information held by the covered entity."[1]

Furthermore, "a compelling motivation for CEs to enact strict HIPAA-compliant security and privacy policies and procedures is the legal community. It can be anticipated that HIPAA-related privacy violation cases against healthcare organizations, insurance companies and business associates will be vigorously litigated."[4]

completely erase all confidential data

user-selectable erasure patterns

Are You in Compliance?

How do you stay in compliance when you perform a Disaster Recovery test at an unsecured, third-party hot site location?

SAE & Fast DASD Erase

In the past, many organizations simply clipped the VTOC at the end of their Disaster Recovery tests at a Hot Site. But erasing test data at the end of a Disaster Recovery test may be one of the most important steps of the test itself. Your data (and its security) is your responsibility; it is not the responsibility of the hot site vendor. Stand Alone Environment (SAE) users enjoy peace of mind knowing they have completely erased all confidential data, thereby safeguarding it from unwanted use. It is also invaluable when decommissioning DASD. The Fast DASD Erase tool not only clips the VTOC; it completely destroys all data.

Government regulations and internal procedures may call for multiple erasure passes. SAE provides user-selectable erasure patterns, allowing users to write a random byte value in addition to binary zeroes across tracks during Fast DASD Erase.

Stand Alone Environment is available for FREE, 30-day trials. It can be downloaded from the NewEra website -- www.newera.com.

Download today at
www.newera.com

Sources

[1] http://www.hipaacomply.com

[2] http://www.hhs.gov

[3] http://www.hhs.gov

[4] http://www.smed.com

Standards for OS/390 System Management

Corporate Headquarters
Morgan Hill, California 95037
800 421-5035
TEL: 408-201-7000
FAX: 408-201-7099
email: info@newera.com