Are You in Compliance?

What Your IT Audit Staff Should Know about HIPAA and GLBA

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 protected health information. The rule requires covered entities to implement administrative, physical and technical safeguards to protect electronic protected health information in their care.*

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 of 1996 (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.

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 electronic protected health information held by the covered entity."

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."

Source: United States Department of Health & Human Services – www.hhc.gov

May 23, 2003 *-- The Federal Trade Commission's Safeguards Rule, which implements the security provisions of the Gramm-Leach-Bliley Act, becomes effective today. As of today, financial institutions subject to the Rule must have in place a comprehensive security program to ensure the security and confidentiality of customer information.*

GLBA – Gramm Leach Bliley Act – 1999

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions.

The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities. Such non-traditional "financial institutions" are regulated by the FTC.

The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, which receive such information. The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions – such as credit reporting agencies – that receive customer information from other financial institutions.

Source: Federal Trade Commission – www.ftc.gov

So, 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?

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. SAE 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

Since its introduction in 1990, Stand Alone Environment (SAE) has become the standard for the repair and recovery of large IBM Enterprise Systems – MVS, OS/390 & z/OS.

Erasing test data at the end of a Disaster Recovery test may be one of the most important steps of the test itself. **Fast DASD Erase** users enjoy peace of mind knowing they have completely erased all test data, thereby safeguarding it from unwanted use. This is especially important in an era of government regulations regarding the protection of personal information. Users also appreciate the reduction in time and money saved during the actual erasure.

SAE Erase Only

SAE Erase Only includes Fast DASD Erase for those users interested in using SAE at their Disaster Recovery tests or when decommissioning DASD.

SAE Full Function

When you need more than just Fast DASD Erase, SAE offers a self-contained, self-loading system software utility that provides immediate access to system datasets through an ISPF-like editor without an active MVS system. The Stand Alone mode of operation used by SAE is absolutely critical during a disaster. Without access to TSO or ISPF, how will you access system files with confidence? How will you diagnose and fix problems? With SAE you avoid this "Catch-22" scenario totally, gaining access to system files and system data with a familiar ISPF-like interface. SAE's commands and services are totally intuitive for systems professionals.

SAE has four unique integrated application in addition to **Fast DASD Erase**. Each of these is of great value to technical staff for building and testing new MVS Images, validating new hardware installations, restoring volumes, individual datasets or members originally backed up using FDR and DFDSS and much more.

Action Services provides complete access to all DASD devices and datasets. Its interface is modeled after ISPF. Users locate critical datasets or members and use specific Action Services to make system repairs. This tool set includes edit, zap, browse, rename, save, delete, undelete, and catalog list/alter.

Restore is simply the fastest way to restore a single dataset. Unlike other backup and recovery systems that require you to restore a complete volume, this application lets you restore a single dataset or member originally created using IEBCOPY, IEBGENER, DFSMSdss or FDR. RESTORE will perform full volume restores from DFSMSdss or FDR if required.

Image Services aids users in the repair of System Images by automatically isolating the components that comprise a specific image. This inspection process is almost instantaneous in identifying the volumes and datasets under investigation. Image Services uses information captured by NewEra Software's IMAGE Focus Inspection Server to pinpoint and provide the means to immediate repair problems.

Hardware configuration allows users to verify hardware installations before bringing the system up.

w w w . n e w e r a . c o m

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

Introducing SAE for VM and VSE

SAE Erase Only is now available for the VM and VSE Platforms. SAE for VM and/or VSE is available on tape only. Call 800-421-5035 to order your trial copy.