



The Best Records Protection You Can Buy.

HIPAA & Business Continuity/Disaster Recovery Overview

What is HIPAA?

HIPAA is the acronym for the "Health Insurance Portability and Accountability Act" of 1996. HIPAA regulations consist of a set of national standards which are designed to force the health care infrastructure to comply with strong security and privacy standards to protect personal health information.

Failure to comply with HIPAA can result in civil penalties (mainly fines) as well as criminal penalties (up to \$250,000 and up to 10 years in prison).

In a recent survey of more than 350 IT leaders in U.S. healthcare organizations, 60 percent consider upgrading security for HIPAA compliance to be their top priority in 2002. Additionally, a recent survey, conducted by Phoenix Health Systems and the Healthcare Information and Management Systems Society (HIMSS), an organization representing more than 13,000 healthcare institutions, revealed that less than 50% of affected healthcare systems have completed an assessment of the effect that HIPAA will have on their organizations.

According to InformationWeek magazine, the final standards will take effect on April 21, 2003, while large health-care organizations have until April 2005 to comply with the regulations. Smaller ones are given an additional year to comply.

Who needs to be concerned with HIPAA?

Obviously, health care providers, health care clearing houses and health care plans are at the top of the list. However, many other types of organizations are not yet aware that they are considered an entity covered by HIPAA. (See box at right.)

Reaching HIPAA compliance represents a huge challenge to many companies. Although the absence of technological specifics regarding how organizations need to go about securing their records may make HIPAA compliance easier in some ways, in other ways, it will be more difficult for covered entities to understand whether they are in compliance.

One measure to be taken which is universally understood is that covered entities must carefully establish security policies and procedures (including Business Continuity and Disaster Recovery plans) and document why they chose certain tactics and technologies to secure their systems.

Any organization that does not display due diligence in starting this process will be in noncompliance. As a word of warning, experts predict that the government will finger a number of non-complying organizations to be "the poster children for HIPAA compliance." HIPAA is not only a technology/information security issue; it's a policy, procedure, and culture change. Change brings opportunity, and HIPAA represents an opportunity for all professionals involved with medical records, not just medical records managers at hospitals, to increase their value to the organization by playing a key role in ensuring HIPAA compliance.

Why is HIPAA an issue for office product buyers?

HIPAA contains strong requirements regarding disaster recovery and business continuity planning. It is therefore essential that covered entities launch the disaster recovery and business continuity planning program in a professional and

straightforward manner. Section -- 142.308 (a)(3) of the Proposed Security Standard requires that

Covered Entities

The below organizations that are included under HIPAA's definition of a "covered entity" (and thusly are required to comply with the law) comprise of the following:

- Indemnity insurers
- Health Maintenance Organizations
- Billing agents that handle activities on behalf of other covered entities

and any organization...

- that transmits health care claims
- that transmits health care payment and remittance advice
- involved with the coordination of health benefits
- that determines health care claim status
- that administers enrollment and disenrollment in a health plan
- that determines and administers eligibility for a health plan
- that administers health plan premium payments
- that administers referral certification and authorization
- that administers first report of injury or health claims attachments

covered entities draft a business continuity/contingency plan, defined in the proposed regulation as “a routinely updated plan for responding to a system emergency,



FireKing fire proof file cabinets carry the UL Class 350 1-hour fire with impact rating, and are available in a variety of sizes and colors.

that includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster.”

One element of the overall contingency plan is a disaster recovery plan; which must contain a process enabling an enterprise to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure. The plan must allow a covered entity to re-create, in the throes of a disaster such as a fire, the entire infrastructure necessary to guarantee information availability.

It's not all about HIPAA compliance, however. It's good business sense - during the course of developing a good disaster recovery and business continuity plan, you are likely to come up with some good information and data needed for high level business strategy decisions, such as determining and prioritizing all your organization's critical business applications.

To state it as simply as possible, the first step in disaster recovery and business continuity planning is records protection. The safeguarding of vital and irreplaceable non-electronic documents is absolutely crucial for HIPAA compliance.

One well-known consultant in the HIPAA community, Michael Miora, CISSP, Founder and President of

ContingenZ Corporation (www.contingenz.com), an international incident management and security consultancy, strongly endorses the use of fireproof containers for the protection of vital records in both hard copy and electronic form, especially in the healthcare industry where HIPAA mandates protection and preservation of health and related information, including signature information contained on consent forms.

“Protection is also relevant for companies outside the healthcare industry that provide some level of self insurance and, therefore, become subject to HIPAA as covered entities or associates,” counsels Miora.

Some potential approaches for protection of vital records include: on-site fire-rated vault, safe or file cabinet, off-site storage at another location of the organization, and storage at a vendor that specializes in off-site vital records storage. Most



FireKing Data Safes are available in a variety of sizes and all carry the UL Class 125 fire and impact rating for 1, 2 or 3-hour protection.

companies employ various combinations of the above approaches. Whether you go with on-site or off-site, the first action to take is to procure fireproof safes and filing cabinets for on-site storage, as you will always, at one point, have vital records on-site, and obviously, no one is able to accurately predict the precise time a business interruption will occur.

Unfortunately, standard filing

equipment is believed to offer fire protection by a large majority of consumers. This thinking, attractive in today's cost-conscious environment because it “seems” cheaper, is erroneous and potentially dangerous. Remember, you're attempting to show potential HIPAA inspectors a “best effort” to protect your most vital information assets, as such it is highly advisable to seek the highest quality.

If you opt to store vital records onsite, it is imperative to seek products that are tested by Underwriters' Laboratory (UL) or other nationally known independent testing labs - absolutely steer clear of equipment with manufacturers' or non-independent ratings. UL, in particular, is the best, as no other testing and standards organization matches their reputation.

One “trick” to be wary of is a product that claims to be “built to” a certain UL class specification claim. This is marketing-driven wordplay, pure and simple - and it leads the customer to falsely believe they are getting a UL rating, but in reality it's just the manufacturer's dubious claim -- UL has never tested it, and how it will stand up to a real fire is anyone's guess. Mark Fulton, a company official at Virtual Insurance, an underwriting firm in South Florida, says his decision to purchase a UL-rated fireproof data safe was fully informed by the UL logo, in fact, Fulton claims that he “doesn't buy so much as a light bulb” unless it is UL tested.

Sources for further info:

- U.S. Department of health and Human Services - www.hhs.gov/ocr/hipaa/
- The International Association of Privacy Professionals - www.privacyassociation.org
- American Health Information Management Association
- Healthcare Information and Management Systems Society - www.himss.org
- Phoenix Health Systems, HIPAA compliance recourses - www.hipaadvisory.com
- Centers for Medicare & Medicaid Services - www.hipaa.org
- ARMA International - www.arma.org