



The Heartbeat of the Hospital

Contingency planning and vital records protection for medical organizations

By Van Carlisle

Most modern medical practices and healthcare facilities – a category that may or may not necessarily include hospitals – already deploy some sort of digital solution for bookkeeping, accounting and office management applications. The trend in the healthcare community tracks with that of the rest of the global economy: Much of the information and data collected will soon be digitally stored and transferred.

The advantages of digitized records management to a medical organization are many. Medical care is delivered within a very data- and information-driven environment, and an Electronic Medical Record (EMR) system is a rapid and efficient method to preserve critical medical information. With increased digitization of vital records, however, there is not a lack of risk involved.

This article focuses on a key single aspect of the digitization of the modern medical organization – the storage and protection of a practice’s vital records, be they digital or paper, in a business continuity context.

The creation and subsequent protection of “backup copies” of a medical organization’s vital records is and always has been a crucial management issue for healthcare providers. When the personal, privileged health information of patients accumulates

The VRP/HIPAA Connection

Vital Records Protection (VRP) is considered by some experts to be a sub-category of business continuity and disaster recovery, and the VRP industry has been rapidly growing during the past few years with both companies and individuals becoming more dependent than ever before on the information they store. Simply stated, vital records and documents are increasingly recognized as the key to survival in the HIPAA era.

HIPAA refers to the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Sections 261-264 of HIPAA require standards to be publicized for the exchange, privacy and security of Protected Health Information (PHI).

HIPAA can apply to health plans, healthcare clearinghouses and to any other healthcare providers who transmit health information. These organizations are called "covered entities." Health plans are individual and group plans that pay for medical coverage. Healthcare clearinghouses include billing services, community health management information systems and re-pricing companies. Healthcare providers include all providers of services and providers of medical and health services as defined by Medicare.

According to Kelly Pierce-Gonzales of KPG Medical-Legal Consulting, "The information that is protected, termed Protected Health Information, or PHI, includes all individually identifiable health information held or transmitted by a covered entity in any form or media, whether paper, electronic or oral."

The majority of healthcare organizations with a HIPAA compliance initiative keep their on-site vital documents and patient records protected confidential by storing them behind two different locked compartments – first in a locked UL-rated fireproof cabinet and then a locked office door.

over the lifetime of a medical practice, the more Vital Records Protection (VRP) becomes a serious issue that, when mismanaged, can not only threaten the livelihood of a practice, it will also compromise the personal information of patients and possibly create a Health Insurance Portability and Accountability Act (HIPAA) violation (see "The VRP/HIPAA Connection" sidebar).

Michael Miora, president of ContingenZ Corporation, a business continuity consultancy, explains, "During the past three years, there have been headlines and lingering stories about healthcare and financial companies that have either lost or compromised data through unprotected backups. Any question about the importance of protecting vital records has been laid to rest by the reputational, financial and legal consequences of such losses and compromises."

Medical practice managers should – and do – prepare for any contingency and unplanned potentially disastrous occurrence by creating backup copies of vital patient records, accounting documents and information from human resources. As the private and sensitive health information of patients, as well as the operational records of a healthcare organization, builds up over the years, the need for better document management and increased protection (VRP, in other words) becomes a crucial component of operations. This provides a measure of insurance that these vital records will not be lost or destroyed in a disaster or some other unplanned business interruption.

Fire, accidental or otherwise caused, is the biggest threat. The most common reason for a document to be unusable after a fire or flood is water damage. The fire suppression systems in most buildings and from the hoses used to extinguish the flames can often cause the most damage to documents if they are not properly protected. Also, if the records are not protected in a UL-rated fireproof container, they will obviously be very vulnerable to destruction during the fire.

HOW TO IMPLEMENT VRP

Some medical organizations may be hesitant to fully convert to digital record storage because of the fear of losing information due to the threat of a virus or the possibility of some sort of system "crash." Documents and records can suffer destruction via any number of ways in a disaster. Hackers, system crashes and actions of malicious or careless employees all drive the fear of a business-shattering loss of vital records if an organization converts to an all-electronic patient record and billing system. This fear, however, is unwarranted if certain business contingency precautions are taken, including regular data backup and protection.

This risk can actually be almost entirely eliminated if the crucial VRP-based precautions are taken prior to any conversion to electronic record storage.

The first VRP procedure to commence is to develop a program and denote responsibility to someone – typically a medical practice manager – classifying all documents and records including paper-based and electronic by degree of their significance to the ongoing operations of the organization, which includes more than just patient records.

Classifications should label records and documents according to the following categories:

VITAL: documents that are irreplaceable

IMPORTANT: not irreplaceable, but could be reproduced only at considerable expense, time and labor

USEFUL: records that, if lost, will cause some inconvenience, but could be readily replaced

NON-ESSENTIAL: records that are in line for routine scheduled destruction

The second VRP measure after classification and categorization is finished is to structure the program for backing up records. Perform backup tasks at least several times per week and every day if feasible. This way, even in the very worst-case scenario, there will be only one day – or just a few days – of lost information in an event that destroys vital records.

Simply classifying and developing a backup program is not enough, however. Once these first two steps are complete, the next and extremely crucial element of VRP occurs when all records labeled vital, important and some useful are secured in a UL-rated fireproof container, typically a data safe or file cabinet.

There are several different practical reasons why a medical



organization's vital records should be stored in fireproof containers. Some of the most important uses of medical records include acquiring proper documentation of a diagnosis and resulting treatment of a patient's health or disease, usage as a means for further clinical research and quality care assessments, providing support for a defense in a possible future litigation, or addressing reimbursement issues with a third party, such as an insurance company.

Regardless of the reasons vital records need to be kept safe from damage, all medical organizations – no matter what type or what size – need to dispense with, as best as possible, the risk of permanently losing these types of records.

WHAT IS NEEDED?

National Fire Protection Association (NFPA) Standard 232, "Protection of Records," recommends that if keeping vital records on site, they need to be stored in a secure, fire-protected location in a fire-resistant file or vault that has been tested by Underwriters Laboratories (UL) or another nationally known independent testing lab. At the end of a predetermined period, two copies of records should be made: one for off-site storage and one for on-site storage, and archival records, such as these backups, should be kept off site.

When researching an adequate on-site fireproof storage device or container for a specific medical practice, one important universal factor is to make sure that the one used is tested and rated by the UL or another nationally known independent testing lab. It is also crucial to procure the correct container for its proposed contents. For example, if most digital data is stored on CDs or Zip drives, it is imperative to use specially designed containers called Media Vaults. These units are small, portable fireproof containers designed to protect patient records stored on CDs, Zip disks, diskettes and microfiche from the damaging effects of heat, humidity, dust and magnetic fields.

Standard filing equipment will definitely not provide the necessary protection from fire or water damage. Even a "fireproof" cabinet will not protect media contained on video tape or digital

disc. It is necessary to use a container specifically designed to protect electronic media.

Since tape and disc media begins to degrade at temperatures of 125° F or humidity greater than 85 percent, in order to be able to guarantee true protection, which is key in offering archival storage, production houses must use equipment that has been tested by Underwriters Laboratory or another independent testing lab and rated to remain at or below 125° F for at least two hours when exposed to fire, as per the Standard Time Temperature Curve, up to 1850° F. You must also consider water from fire hoses, sprinklers and burst pipes, as that is where the interior relative humidity less than 80 percent standard becomes crucial.

Other things to emphasize include the storage room environment, which should be climate controlled at 63° F and 35 percent relative humidity, and physical security, with restricted access measures that ensure the room where the container(s) are kept only be accessed upon proper authority and supervision.

Even if a medical practice deploys an off-site record storage solution, i.e. from specialized records storage and records management solutions provider, it is certain that at some point any active medical practice will have vital records on site and a need to protect them.

Miora says, "While off-site storage of encrypted vital records is a necessary and accepted best practice, it is no substitute for maintaining useful, live information locally (on site) in containers that are appropriately resilient."

Risk management policies must be established and put into action long before an emergency arises. A critical component in the risk management strategy of any medical office must include an on-site UL-rated fireproof filing cabinet or container for the storage and protection of vital records such as, patient information, X-rays, employee records, licenses and important billing documents.

Specific medical record retention laws vary from state to state and change depending on the exact type of record. The American Health Information Management Association (AHIMA) is the organization created to assist the healthcare industry when it

comes to gathering, managing and storing medical records. A doctor's office will have rules and regulations regarding VRP imposed on them by the state in which they operate. AHIMA only makes guidelines or recommendations, and then each state decides to fully accept, slightly alter or completely disregard the guidelines for their own individual legislation.

For example, a state might require that paperwork regarding the specific information surrounding a patient's treatment be retained for 10 years after the patient is discharged. Or that same state could enforce an indefinite retention period for documents, such as surgical records, birth certificates or death certificates. Some organizations may take the additional measure of drafting broad-based "blanket" retention policies regarding all vital records or documents, not just medical records.

Simply put, the need for medical organizations to better manage vital records has increased dramatically over the past few years. Gain an understanding of this issue now to figure out the best set of vital records protection solutions for your practice.

About the Author

Since 1975, Van Carlisle has been the president and CEO of FireKing Security Group (www.fireking.com), an asset protection company in New Albany, Ind. Questions and comments may be directed to editorial@contingencyplanning.com.

For More Information

National Fire Protection Association
www.nfpa.org

Underwriters Laboratories Inc., Fire Protection Division
www.ul.com/fire/

The American Health Information Management Association
www.ahima.org

Kelly Pierce-Gonzales of KPG Medical-Legal Consulting, Inc.,
(915)252-3044
www.kpgmlc.com

Michael Miora, President of ContingenZ Corporation
www.contingenz.com