

FOR THE RECORD

Vital Records **Protection**

for the Physician Practice

(Proper steps should be taken to ensure that medical records are protected against fire and other catastrophes.)

By Van Carlisle

Every type of organization generates a number of documents (both paper and digital) that are special or important enough to safeguard from catastrophic disaster, whether caused naturally or otherwise. Some entities make the decision to protect these documents, a concept known in legal terms as vital records protection (VRP), in hopes of having a smoother recovery in the event of a business interruption such as a fire, flood, or other disaster.

In many cases, facilities are motivated to launch a VRP program by their insurance provider. Other industries or categories of businesses are additionally required by law or governmental regulations to provide adequate VRP.

Regardless of the driving motivation, having a detailed, written set of policies dealing with VRP is a generally acknowledged best practice for any organization that gathers and stores information and data. Especially in the aftermath of events such as the September 11 terrorist attacks, constant updating and revision of VRP plans are becoming necessary. A business continuity and disaster recovery strategy is only as strong as its ability to protect vital data.

VRP and HIPAA

The health information field is the most obvious profession subject to VRP policy requirements such as those mentioned above, including, but not limited to, records protection guidelines set forth under HIPAA. Patient records (digital and paper), employee information, and insurance documentation are some of the documents that are legally categorized as vital records, which covered organizations should be protecting from disaster at all times. 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 that is universally understood and relatively simple to comply with 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 noncomplying organizations to be “the poster children for HIPAA compliance.”

It is worth noting that HIPAA is not only a technology/information security is-

sue, it's also 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.

Standards Organizations

American Society for Testing and Materials

100 Barr Harbor Drive
P.O. Box C700
West Conshohocken, PA 19428-2959
www.astm.org

National Fire Protection Association

1 Batterymarch Park
Quincy, MA 02269-9101
www.nfpa.org

Underwriters' Laboratory

333 Pflingsten Road
Northbrook, IL 60062-2096
www.ul.com

Various Approaches to VRP

Some potential approaches for protecting vital records include off-site storage at another location of the organization, storage at a vendor that specializes in off-site vital records storage, and an on-site fire-rated vault, safe, or file cabinet system. Out of necessity, the majority of medical organizations employ various combinations of these approaches. Whether the decision is made to go with on-site or off-site storage, the first step is to procure fireproof safes and filing cabinets for on-site storage. An active medical organization will always, at one point or another, have vital records on site, and, obviously, no one can accurately predict the precise time a business interruption or disaster will occur.

Some offices fulfill these VRP requirements by sending the records to off-site locations with ample fireproof storage; other medical offices use more cost-effective on-site VRP. Brenda Laws, office manager at E.H. Perez, MD, in Ashville, N.C., explains the situation in her office.

“We were storing our electronic medical records duplications at an outside storage company,” Laws says. “That was turning into a hassle and becoming very expensive, so we looked into using a fireproof safe to store records on site. The safe has not only saved us money, but it has also made getting access to our non-current files much easier and faster, allowing us to better help our patients in regards to their medical records.”

There are several practical reasons why patient records can be stored in on-site fireproof containers. Some of the most important uses of medical records include securing proper documentation of a doctor's diagnosis and subsequent treatment of a patient's health or disease, serving as a tool for further clinical research and quality care assessments; providing a defense in possible future litigation; and addressing reimbursement issues with a third party such as an insurance company. Regardless of the reasons they are kept safe from fire, all doctor's offices—no matter the size—need to eliminate, as best as possible, the risk of permanently losing these types of records.

For vital records that are on site—whether temporarily or otherwise—a majority of consumers believes standard filing equipment offers enough fire protection. This thinking, attractive to management because it seems cheaper, is erroneous and potentially dangerous. Remember, you are attempting to protect the organization's most vital information assets, and it is highly advisable to seek the highest quality of protection. Price should not be an overriding factor in the decision. It is imperative to seek products that are tested by Underwriters' Laboratory or other nationally known independent testing labs. Absolutely steer clear of equipment with manufacturers' or nonindependent ratings. No other testing and standards organization matches Underwriters' Laboratory's reputation.

One “trick” to be wary of is a product that claims to be built to a certain Underwriters' Laboratory class specification claim. This is marketing-driven wordplay and it leads the customer to falsely believe they are getting an Underwriters' Laboratory rating, but in reality it's just the manu-

facturer's dubious claim. Underwriters' Laboratory has never tested it, and how it will stand up to a real fire is anyone's guess.

One thing to consider is the fact that VRP does not start and finish with patient records. Additional categories of recorded data in a medical organization that typically fall under the category of vital may include the following:

- contracts/agreements that prove ownership of property, equipment, vehicles, products, etc;
- operational records such as current or unaudited accounting and tax records, current personnel and payroll records, client account histories, and shipping delivery records;
- current vendor files;
- current standard operating procedures; and
- produced reports and summaries.

The above list should be considered a basic starting point. Also consider that although a specific category of records may not be deemed vital, it does not automatically mean that type of record is not worth protecting. Each type of record must be analyzed and tiered to determine the amount of protection you should provide. If not vital, you may determine nonvital but valuable records to be classified as:

- 1) Important: not irreplaceable but could be reproduced only at considerable expense, time, and labor;
- 2) Useful: records that, if lost, will cause some inconvenience but could be readily replaced;
- 3) Nonessential: records that are in line for routine destruction.

To validate the classifications, those responsible for the vital records program should interview the managers and personnel who create records. Fortunately, you do not have to implement this crucial element of the business continuity/disaster recovery plan in a vacuum. There are a number of standards bodies and organizations, most of which have a healthy amount of information publicly available on the Internet. The standards apply not only to the vital records themselves, but the actual facility and vaults housing the vital records and data recovery equipment as well.

The AHIMA assists 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. The 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.

Kevin Gould, director of public relations at the AHIMA, comments on how medical facilities of all sizes should protect backup documents and files as best as possible, saying, "Your backup plan should include where and how backups will be stored. Backups will be useless if they are destroyed in a widespread disaster such as a fire. You should consider storing backups some place other than near your computer. Alternatives include such simple options as a fireproof container or file cabinet. You may also choose to store your backups off site in a secure location."

As noted, specific medical record retention laws vary from state to state and change depending on the exact type of record. For example, a state may require that paperwork regarding the specific information surrounding a treatment given to a patient should 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, and death certificates. Some medical facilities even go as far as to create blanket retention policies regarding all records or documents, not only medical records.

Keeping vital records anywhere other than a fireproof filing cabinet or safe is a risk no medical office should take. Until legislation is passed to require fireproof record storage in every state, it is up to each office to fireproof their record storage. Taking the proactive step to eliminate the risk of permanently losing medical records can prove to be a major time, effort, and money saver.

— Van Carlisle is president and CEO of FireKing.