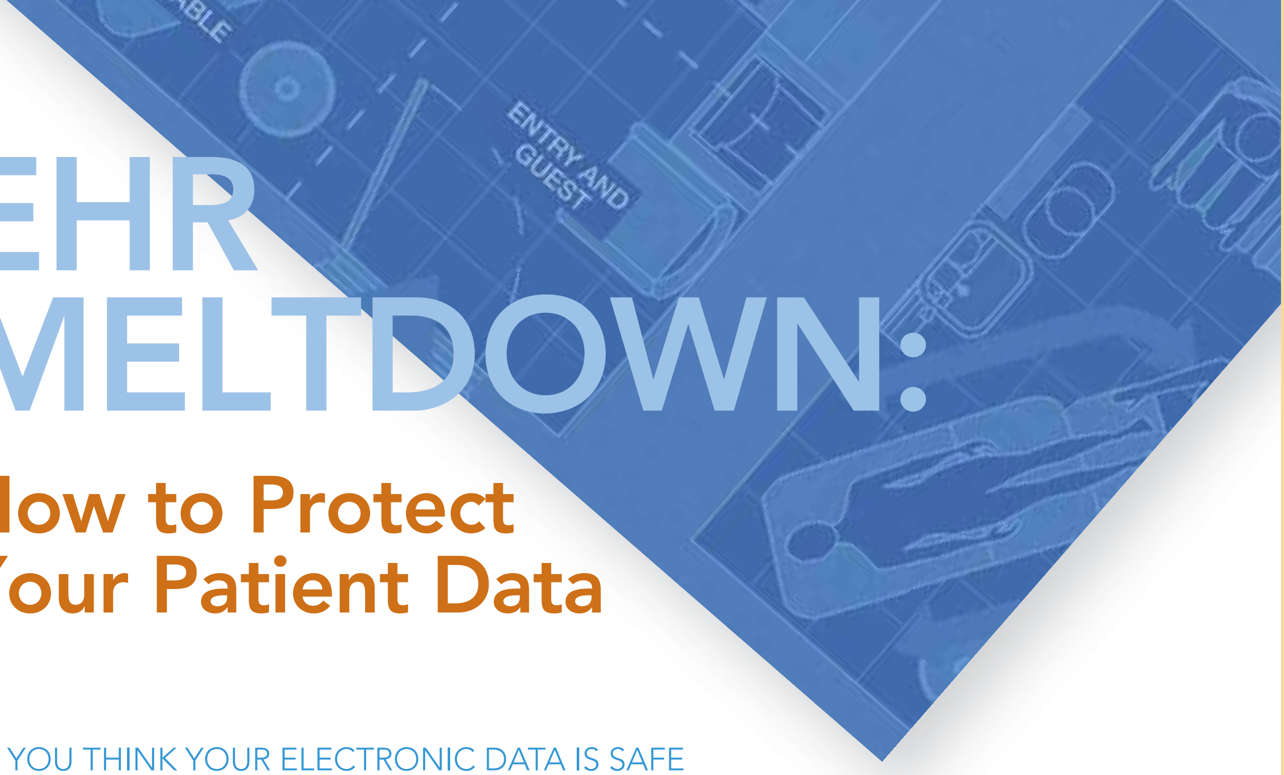


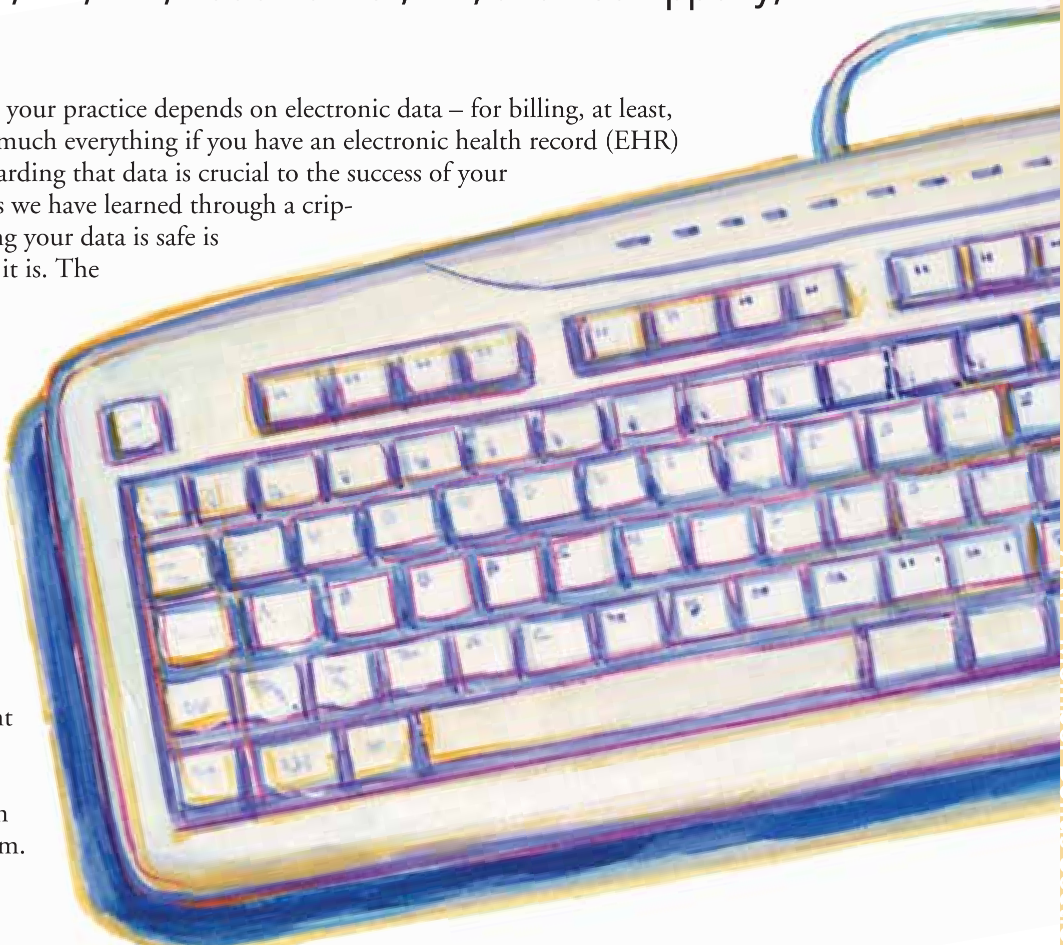
EHR MELTDOWN:

How to Protect Your Patient Data

DO YOU THINK YOUR ELECTRONIC DATA IS SAFE JUST BECAUSE YOU HAVE A BACKUP PLAN IN PLACE? THESE AUTHORS FOUND OUT HOW WRONG THAT CAN BE.

T. Eric Schackow, MD, PhD, Todd Palmer, MD, and Ted Epperly, MD

Chances are that your practice depends on electronic data – for billing, at least, and for pretty much everything if you have an electronic health record (EHR) system. Safeguarding that data is crucial to the success of your practice. But as we have learned through a crippling loss of data, thinking your data is safe is not the same as knowing it is. The purpose of this article is to describe how our loss came about, what we learned from it and, most important, how to prevent this from happening to your practice.



The meltdown

The Family Medicine Residency of Idaho (FMRI) is an independent freestanding corporation affiliated with the University of Washington Residency Network system. FMRI comprises more

AAFP Member Bonus Section

TOM FOTY

Due to our flawed backup scheme, our most recent recoverable data set was now four months old.

than 60 providers (family medicine residents, faculty physicians and midlevel providers) handling over 46,000 outpatient visits per year at two clinic sites. When our meltdown occurred, we were about seven months into our EHR implementation and had been documenting essentially all outpatient visits in our EHR for more than four months.

We had been informed that the industry standard was to perform a partial backup each night and a complete backup (during which the system is unavailable) weekly, and these were the instructions given to our IT director. We believed that the backups were occurring, but we did not verify this. In fact, no complete backups were performed for a period of four months, and we didn't realize this until after we suffered a power outage one night at about 2 a.m.

An uninterruptible power supply (UPS) was automatically triggered; it could keep the EHR database server powered for 45 minutes. Due to misconfiguration errors, however, warning systems did not function properly, an orderly shutdown process was not initiated, and the server ran until the UPS battery was exhausted. The sudden, disorderly power loss to the server resulted in severe corruption of our EHR database. All of our data was still on the hard drives, but it had been garbled and was rendered unreadable. And due to our flawed backup scheme, our most recent recoverable data set was now four months old.

Approximately 12,000 patient visits worth of information was lost. Worse, as part of our EHR implementation, we had done much preloading of patient information during the lost four-month period. Literally thousands of hours of provider and nursing time had been spent to enter medication and problem lists, allergies, immunizations, past medical and social history, clinical summaries and visit notes. All of this information was presumed to be lost, and the initial response from our software vendor was that it was most likely nonrecoverable.

■ Through the loss of four months of data, the authors learned the importance of data protection systems.

■ While most of the lost data was eventually restored, the process was lengthy and expensive.

■ The practice formulated a plan that maximized data availability and security through redundancy of systems, accountability and transparency.

Our immediate reaction

We quickly set out to do everything in our power to attempt to recover the lost data. We shipped our EHR server's hard drives across the country to a company that specialized in data recovery. Our most pressing challenge, though, was to continue providing quality clinical care with four months of clinical data unavailable to us. We used every resource we could to piece together the recent clinical history. All patients were given a handout in the waiting room, informing them of the data loss and asking them to fill out a questionnaire that gave us pertinent recent clinical information. We frequently called pharmacies to acquire current medication lists. Being a residency training program, we were fortunate to have Medicare teaching forms that had been filled in by our faculty. These gave us problem lists, assessments and plans, and physical exams for the more complicated patients.

The event seriously affected all areas of our program. Good communication through clinic-wide meetings and frequent e-mails did

About the Authors

Dr. Schackow is associate program director of the Saints Mary & Elizabeth Medical Center Family Medicine Residency in Chicago and clinical assistant professor in the Department of Family Medicine, University of Illinois at Chicago. Dr. Palmer is faculty coordinator of the informatics curriculum at the Family Medicine Residency of Idaho and a clinical assistant professor in the Department of Family Medicine, University of Washington, in Seattle. Dr. Epperly is CEO and program director of the Family Medicine Residency of Idaho, clinical professor of family medicine at the University of Washington School of Medicine and president-elect of the AAFP. Author disclosure: nothing to disclose.

BACKUP AND THE ASP-HOSTED EHR

What if your EHR is hosted by an application service provider (ASP)? In such a case, the EHR database is maintained by a remote off-site provider, while the physician connects to both the EHR application and the data via the Internet. Safeguarding EHR data and maintaining high EHR availability are no less important in this arrangement; our five values and three dimensions of data protection are equally applicable to these situations. The primary difficulty is that the values of *accountability* and *transparency* are considerably more difficult to maintain. If the ASP is highly competent and conscientious, EHR data may actually be safer in their hands than in the hands of novice on-site practice personnel. On the other hand, if the ASP is not reliably implementing our three dimensions of data protection, EHR data may be compromised. Finally, reliable Internet connectivity to the ASP has the potential to become an unpredictably weak link in the chain.

A well-written contract between the ASP and the practice should stipulate specific standards for safeguarding of EHR data. However, a contract by itself does not guarantee the availability of the data; it only provides the physician with means for legal and perhaps financial remedies in the event that it can be proven that an ASP's loss of EHR data was the result of its failure to honor the terms of the contract. A difficult court battle and a cash settlement would provide little consolation for most family physicians, who would much rather have their intact EHR data restored. Therefore, the only way to ensure that data is safeguarded is to physically have a copy of the data. We suggest a provision in ASP contracts stipulating at least biweekly data downloads from the ASP to the local practice site, thereby allowing physicians to regularly inspect their own data and further secure it locally as they see fit. Unfortunately, the lack of a locally installed EHR application may still render this data inaccessible (and therefore unavailable for use by the physician) in the absence of a connection to the ASP's software.

a lot to maintain morale and to give staff support and direction in dealing with patients, third-party payers, other physicians' offices and attorneys who requested records related to care provided during the loss period.

Fortunately, 11 weeks after our data meltdown, we were able to recover nearly 100 percent of our data. This was the result of a lot of hard work by many people internal and external to our residency program – and a fee of more than $10,000 paid to the data recovery firm. The experience also taught us a lot about the safekeeping of electronic data, and it taught us that we never want to go through anything like it again.

Lessons learned

Computerized practice management and EHR technology have hidden costs, including the price of appropriately protecting data. But these costs are far less than the expense of being forced to scale back or shut down a practice because of a system failure. A high degree of reliability in EHR server hardware is certainly desirable, but as we learned, even highly reliable systems eventually fail. It is not a question of whether a system will fail, but how, when and whether we are prepared to manage the consequences.

For the future, we realized one central goal needed to be the ability to have our EHR system running again within one day following a failure like the one we experienced. And "within one day" was a worst-case scenario; all of our systems needed to be designed to further minimize potential downtime and maintain access to our data.

We used five values to guide our discussion as we set out to formulate a data protection plan:

1. Availability. Because of the mission-critical nature of our work (full-scope outpatient and inpatient family medicine, including obstetrics), we believed that our data should ideally be continuously available 24/7/365 – even in the event of data loss, data corruption or equipment failure. System downtime needed to be minimized. We also needed to broaden our thinking to consider various adverse conditions, including but not limited to an extended regional power outage that might last seven days, burglary, fire, flood and other natural disaster.

2. Redundancy. Increased redundancy – having multilevel, overlapping systems that work both synchronously and in isolation to protect our data while allowing us access to it – should theoretically lead to higher availability.

3. Security. Clearly, our data should always be secured against unauthorized access (theft,

They realized the importance of regular backups, distributed storage of backups, and multiple methods of data protection.

They emphasize the importance of accountability in the backup process and verification that backed up data can be successfully restored.

IMPLEMENTING A THREE-DIMENSIONAL BACKUP PLAN

We now have what we consider a reasonably bullet-proof data-protection scheme. Here's an outline of how you might go about building a similar arrangement. We won't go into technical details here, assuming that most practices would turn to technical consultants or IT staff for implementation:

1. Make sure your EHR server has a fault-tolerant disk storage system and redundant hardware: power supplies, internal server hardware and external uninterruptible power supplies (UPSs).

2. Incorporate software that allows your UPSs and servers to communicate for graceful shutdown of the EHR server in the event of power loss prolonged enough to exceed the battery capacity of the UPSs. The software should be able to telephone, page and e-mail alerts whenever a UPS is activated. Test the connections and software weekly.

3. Add a "warm-spare" server ready to accept restored EHR data. This can also function as the "test-restore" server when testing the viability of your backup media (see point 21 below). Our warm spare is on-site, but some practices may choose to position it off-site.

4. Consider adding a "mirrored" EHR database server (a server connected to the main EHR database server and maintaining a continuously updated duplicate copy of the running database). We have not gone to this length, but large practices able to manage the extra complexity and expense may want to incorporate mirroring.

5. Every night, perform "warm" tape backups (backups performed while the server is still on with the database running). These may be either incremental (capturing only changes since the most recent backup) or complete.

6. Every week, perform "cold" tape backups (backups performed while the database is temporarily shut down and the EHR is inaccessible). These are complete database backups, never incremental.

7. Follow a standard Grandfather-Father-Son (GFS) tape backup and rotation strategy, which requires at least 21 tapes or tape sets:

- Five are labeled as Daily tapes (sons), *Monday* through *Friday*.
- Four are labeled as Weekly tapes (fathers), *Week 1* through *Week 4*.
- Twelve are labeled as Monthly tapes (grandfathers), *January* through *December*.

If a full backup exceeds the capacity of one tape, create a "tape set" according to the method detailed in your tape backup software.

8. Beginning on a Saturday, perform a full, cold backup to the *Week 1* tape.

9. Also on Saturday, copy essential patient information (demographics, problem lists, medication lists, allergies, etc.) to rewritable CD or DVD media in a form that can be read on a laptop. (We use a specially designed database process to extract this data in an EHR-independent file format that can be read by Microsoft Office programs such as Excel and Access.) The advantage of this "essential data" on CD/DVD is that it is a simple, robust method to ensure continued read-only access to most relevant patient information in the event of any prolonged EHR catastrophe. Perform this type of backup biweekly.

10. Beginning the following Monday, perform daily warm backups on the daily tapes. *Monday* should be a complete backup, while *Tuesday* through *Friday* may be incremental backups. Store the daily tapes on-site.

11. Once a week, print paper appointment schedules for the next three weeks.

12. On Saturday, perform another full, cold backup on the *Week 2* tape.

13. Continue with this rotation method until the last day of the month. On the last day, no matter what day of the week it is, perform a full, cold backup on the first monthly tape. Label the tape with the current date.

14. Continue the rotation through all 12 months of the year.

15. The monthly tapes can be archived for permanent storage or recycled on a quarterly, yearly or biannual basis. If desired, additional backups can be performed every quarter or every year for long-term archiving.

16. Set the backup software to follow every tape backup, whether warm or cold, with intrinsic verification of the accuracy of the backup.

17. Encrypt data in the process of backup to mitigate risk of theft, loss or tampering (unauthorized access).

18. Store backup media in plastic cases with a paper seal applied over the case opening to further mitigate the risk of tampering, and keep them in secure locations (specially locked cabinets or a safe, depending on the location).

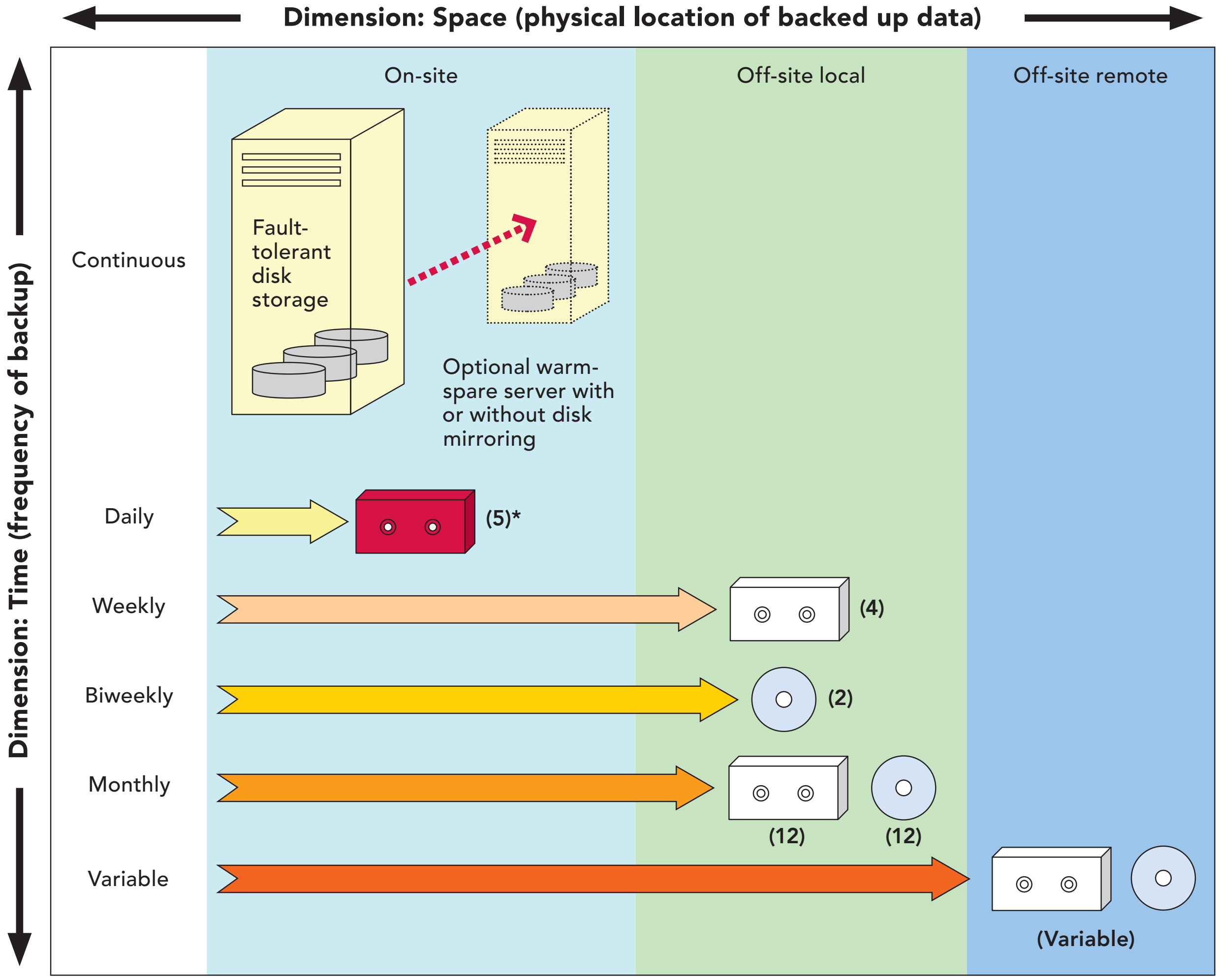
19. Arrange to store weekly and monthly backup media in a local off-site location. (We have a shuttle that travels between clinic sites; it shuttles batches of tapes back and forth weekly.)

20. Periodically, rotate off-site backup media to a remote (out-of-county) location. You might, for instance, want to do this for longer-term archiving.

21. Every week, perform a "test restore" of the database from randomly selected backup media, restoring the data to your warm-spare server and then testing to ensure that the EHR can properly access the restored data.

22. Maintain logs of all backup activities, and require that they be signed off by supervisory personnel who verify adherence to backup procedures.

23. Arrange for an independent outside audit of your backup system every six months.


Dimension: Space (physical location of backed up data)
Dimension: Time (frequency of backup)
On-site
Off-site local
Off-site remote
Continuous
Fault-tolerant disk storage
Optional warm-spare server with or without disk mirroring
Daily
(5)*
Weekly
(4)
Biweekly
(2)
Monthly
(12)
(12)
Variable
(Variable)

* Numbers in parentheses refer to the number of tapes, disks or backup sets needed.

Dimension: Method (protection/recovery method)

Fault-tolerant disk storage: Storage designed to work properly even after partial failure.

Warm-spare server: A server installed and ready to take over from the primary server in case of failure.

Server mirroring: The simultaneous use of two or more servers each maintaining system data.

🟥 **Warm backup:** A backup run while the system is in use; may miss backing up some open files.

▭ **Cold backup:** A backup run while the system is inaccessible to users.

○ **Extract to optical media:** A read-only copy of crucial data in a form accessible even if the EHR is down.

The authors believe that everyone in the practice should know enough about the data protection plan to be confident in the security it offers.

The data protection plans and procedures outlined here should be applicable to any practice data.

The elaborateness of a practice's backup plan will naturally vary with the size and resources of the practice.

intrusion, malicious tampering, etc.). While data security in this sense is beyond the scope of this article, we recognized that we needed to broaden our thinking to include security as it related to our data backup systems (for example, theft of a backup tape from an individual's car or home was a possibility that needed to be protected against). Increasingly redundant systems can theoretically lead to additional avenues for security breaches.

4. Accountability. We believed that everyone should be accountable when it comes to data protection and disaster preparedness. Statements such as, "That's the responsibility of the IT department," or, "I *think* they're backing up the data," became unacceptable. This also included holding the backups themselves accountable, so to speak. In other words, the backups needed to be actively verified in such a way that proved that the data was retrievable and usable.

5. Transparency. We believed that everyone in our organization should have at least a basic overview of the steps being taken to accomplish the above objectives. Naturally, certain details would not be made public for security reasons, but we felt that transparency was imperative to regain and maintain the trust of our physicians, our employees and our patients. All of these stakeholders had invested large amounts of time and effort into working with our EHR, and they needed to be reassured that their work would never again be damaged or destroyed.

Next, it was clear that the oft-quoted and well-meaning (but vague) directive given by EHR vendors to physicians, "Make sure that you back up your data!" needed some additional clarification. We thought we were doing this from the start, and yet a deadly combination of ignorance and complacency put us in a dangerous predicament. We realized that our data needed to be protected in three different dimensions: *time*, *space* and *method*. In other words, data backup needed to occur at multiple times, backup media needed to be secured in different locations, and different backup methods needed to be employed.

Keeping the above five values and three dimensions in mind, we implemented a series of policies designed to safeguard our data and keep it continuously available. The various steps are detailed in "Implementing a three-dimensional backup plan," page A6. Two critically important points are worth highlighting. First, we now verify that backup tapes are indeed viable by pulling specific tapes from all areas of the backup scheme at least weekly and doing a true test-restore to a spare server. The test restore is the only way to definitively document that backup media will be helpful in an emergency. And second, we no longer assume that backups are being performed correctly by a single individual; rather, we enforce an accountability process which ensures that more than one person is monitoring our data protection procedures.

More work to do

In this article, we have chosen to focus exclusively on protection of the EHR database. However, we feel that the general principles outlined above can be successfully applied to most databases relevant to a family physician's practice. Attention to the five values and three dimensions of data protection will go a long way toward preparing a practice to weather the storms of unexpected system failures.

We recognize that the principles we have outlined in this article are neither perfect nor exclusive of other solutions. They simply constitute our best efforts to understand and address this problem. We are still working out the implementation details in our own plan, and we will no doubt need to make changes as we go. Physicians will need to customize their approaches depending on their own individual tolerance for data loss and EHR downtime, cost constraints ("high availability" systems tend to incur extra expense) and access to knowledgeable IT personnel. Some practices may choose to adopt procedures that are less complex and less costly than ours, while others may choose to be even more stringent.

During our EHR database crisis, open communication and venting of frustration were critical. Accountability, transparency and daily communication were paramount. A sense of "we are all in this together" and a positive, proactive attitude of "getting through this and becoming stronger by it" permeated our culture. In fact, it was this attitude that led to the writing of this article, so that others do not repeat our mistake. FPM

Send comments to **fpmedit@aafp.org.**