# Educating the Medical Community About Medical Information Security*

**by M. E. Kabay, PhD, CISSP**
**Associate Professor, Information Assurance**
**Program Director, Master of Science in Information Assurance**
**Division of Business and Management**
**Norwich University, Northfield, VT 05663-1035 USA**

**Version 21 – May 2004**

## 1 Security in the Medical Context

In today's rapidly changing world of health maintenance organizations, telemedicine, computerized patient records, close linkages between medical-care delivery and insurance companies, security of medical information is growing in complexity and importance. Multidisciplinary teams take care of an aging population; litigation is at an all-time high in the United States; and governments, professional bodies and accreditation organizations all concur that the security of patient information — and even of information about care-givers — must be safeguarded. Medical informatics — the high-tech handling of medical information — has become a challenging new specialty of information-technology management.

This White Paper summarizes some of the key issues of medical information security and is intended to spark discussion and generate comments for improvement.

## 2 Fundamental Concepts of Information Security

The fundamentals of information security are constants, but circumstances alter their relative importance. The following summary is adapted from sections of *The NCSA Guide to Enterprise Security* by M. E. Kabay (McGraw-Hill, 1996; ISBN 0-07-033147-2).

### 2.1 The Mission of INFOSEC

The classic definition of information security is drawn from IBM Corporate Policy Number 130 in the 1970s:

Data security ... [involves] the protection of information from unauthorized or accidental modification, destruction and disclosure."

* This White Paper was first published in 1997 under the auspices of the National Computer Security Association (NCSA, later ICSA and then TruSecure) when the author was Director of Education of the NCSA. The author has made minor changes over the years to update the content.

 

Another *classic triad* names confidentiality, integrity and availability. Donn B. Parker, a respected author, teacher and thinker in the security field and formerly a principal in the SRI high-tech consultancy, has added to this triad the concepts of possession, authenticity and utility. These six fundamental and irreducible components of information security are sometimes called the *Parkerian Hexad.*

## 2.2 Definitions

*Protection* means reducing the likelihood and severity of damage. Another way of putting this is that information security strives to reduce risks. It is not possible in practice to provide perfect prevention of security violations. Common sense suggests that the degree of protection must match the value of the data.

Information is protected by caring for its form, content and storage medium.

*Unauthorized* means forbidden or undocumented. The very concept of authorization implies classification: there must be some definition of which data are to be protected and at what level.

*Accidents* account for a major proportion of data damage. Accidents are due mostly to ignorance or to carelessness. Management must either hire well trained, knowledgeable staff or provide appropriate on-the-job training. In either case, part of the task facing all managers is to create, maintain and enhance motivation to do a good job. These basic management issues profoundly affect enterprise security.

*Modification* means changes of any kind. The ultimate modification is *destruction.* However, you can usually spot destruction fairly easily. With adequate backups copies, data can be restored quickly. A more serious problem is small but significant changes in data. The work required to find the changes is often a greater problem than the changes themselves. Computer viruses that wipe a hard disk identify themselves at once and can be removed quickly. Viruses that make small random changes can persist for months, ruin the integrity of backups, and end up costing the victim more than the virulent disk destroyers.

*Disclosure* means allowing unauthorized people to see or use data. Again, this word implies the need for a system of data classification. Who can see which data and when? This is a particularly important issue for medical informatics.

*Confidentiality* is a wider concept than disclosure. For example, certain files may be confidential; the data owner may impose operating system controls to restrict access to the data in the files. Nevertheless, it may be possible for an unauthorized person to see the names of these files or find out how often they are accessed. Changing a file's security status may be a breach of confidentiality. Copying data from a secure file to an unsecured file is a breach of confidentiality. When a supervisor at a Florida clinic stole the list of HIV+ patients and used it to tell people in bars whether to go out with individuals based on their status, he committed a breach of confidentiality. Another confidentiality issue is the growing concern over sharing medical information with insurance companies and health-maintenance organizations.

 

*Possession* means control over information. When thieves copy proprietary software without authorization, they are breaching the owner's possession of the software. When two security guards at a different Florida clinic stole a pair of PCs containing the names and addresses of 4,000 people registered as HIV+, they caused a breach of possession; in fact, they never did breach confidentiality because they reformatted the hard drives without looking at the contents.

*Integrity* refers to internal consistency. A database is termed structurally corrupt when its internal pointers or indexes no longer correspond to the actual records they point to. For example, if the next record in a group is in position 123 but the index pointer refers to position 234, the structure lacks integrity. Surreptitiously using a disk editor to bypass security and alter pointers in such a data structure would impair integrity even if all the data records were left intact. Logical corruption occurs when data are inconsistent with each other or with system constraints. For example, if the summary field in an patient record claims that the patient has been under treatment for 20 days when the individual treatment records clearly show a total of only 5 days, the data structure is logically corrupt; it lacks integrity.

*Authenticity* refers to correspondence between data and what the data represent. For example, if a field is supposed to contain the ID of the current treating physician, it should not informally be used to show the ID of the nurse in charge of the unit. Another example is electronic mail fraudulently sent in the name of a hospital administrator; the only breach of security in such a case is loss of authenticity.

*Availability* means that data can be gotten to; they are accessible in a timely fashion, convenient, handy. If a server crashes, the data on its disks are no longer available; but if a mirror disk is at hand, the data may still be available. When a nurse in the ICU cannot access a patient record within seconds because the local area network is clogged with traffic because the medical students are playing interactive games on the network, the nurse is experiencing a problem in availability. Smart cards have been proposed to carry large amounts of a patient's recent medical history as a method of increasing availability of information in an emergency even if the person is unconscious.

*Utility* refers to the usefulness of data for specific purposes. Even if the information is still intact, it may have been transformed into a less useful form. Parker gives as an example the unauthorized conversion of monetary values in a database; seeing employees' salaries in foreign currency reduces the utility of the data. One of my colleagues was called in to help a firm whose source code had all been encrypted by a departing programmer. The programmer claimed to have done so to protect his ex-employer's security, but unfortunately claimed to have forgotten the encryption key. In a formal sense, the data were authentic, accurate and available--they just were not useful.

# 3 Legal and Professional Requirements for Medical Information Security

Both historical standards of medical ethics and modern legal requirements impel everyone involved in health care to safeguard the security of medical records. In the United States, federal regulations explicitly require agents of the federal government to protect medical confidentiality. State laws vary in the degree of protection afforded patients. The Joint Commission on

 

Accreditation of Healthcare Organizations (JCAHO) publishes extensive guidelines that include sections on information management. Failure to conform to these minimal standards of information security may lead to withdrawal of JCAHO accreditation. In addition, civil law in most jurisdictions permits patients and anyone else affected by failures of information protection to sue in civil court for redress; individual administrators, physicians, nurses and other staff may be named in such lawsuits.

# 4 Impediments to Medical Information Security

Security experts concur that corporations and government have only partly succeeded in implementing even modest programs for information security. However, in my experience in large metropolitan hospitals, I have found a generally poor level of security even by the meager standards of industry and commerce. There seem to be relatively few full-time information security specialists working in the medical field; security awareness programs are few; and health professionals and medical administrators seem relatively unconcerned about the issues.

In a case reported in February 1997 from Sheffield, England, a hospital handed over 50,000 confidential gynecological records to a data processing firm that hired people off the street and set them to work transcribing the unprotected data. The scandal resulted in withdrawal of the contract, but thousands of records were exposed to a wide variety of people with no background checking to ascertain their reliability.

What accounts for such cavalier attitudes? In the absence of thorough survey and interview data to study this question, we can only surmise that several factors contribute to this lackadaisical attitude. The following sections suggest areas that would benefit from thorough study but that can reasonably be expected to play a role in determining the behavior of medical personnel.

## 4.1 Inapplicability of Normal Modes of Identification and Authentication

### 4.1.1 Normal Logon and Logoff Delays are Intolerable

Urgency of data access accounts for a good deal of the characteristic impatience of medical staff for attempts to implement security.

The medical environment in clinics and hospitals imposes a responsibility for rapid response to medical emergencies; in some cases, seconds can make the difference between life and death. Staff in intensive care units and the emergency room cannot afford to waste time logging on and off hospital systems in order to protect confidentiality and integrity.

In addition to the required speed of information access, medical personnel also have to share systems that are used for many brief sessions; one member of the treating team may have to use the terminal or workstation for a minute to enquire about one patient or a lab result, then another person has to do the same for a different patient.

A typical logon and logoff take at least 30 seconds; if a network is slow, the wait can extend to over a minute. Few medical personnel could tolerate the repeated delays caused by their episodic use of their computer systems. In the aggregate, insisting on such logon/logoff cycles

 

for every request for every person would add to the already heavy load on overworked personnel and very likely increase the likelihood of errors in patient care.

### 4.1.2 Unprotected Workstations

The typical response of medical staff to their need for high availability is to let the first user of a terminal or workstation log on in the morning to patient records and simply not log off thereafter. I have seen terminals at hospitals and clinics that have not had a logoff since the last time the network went down.

Many of the terminals and workstations in the medical environment are not protected against unauthorized consultation or even unauthorized modification of medical and administrative data. Workstations seem to lack screen savers that would blank the screen after a minute of inactivity; even those that have screen savers seem to have the password disabled.

There have been cases of unauthorized read-access to patient records because of such weaknesses in security policies. For example, in one case, an orderly called an attractive patient at home after her discharge. When the offended patient demanded to know how the orderly had obtained her home number, he answered guilelessly that he had looked it up on an unattended terminal at the nursing station on her floor. In another case, a psychologically disturbed member of the cleaning staff used an unattended terminal to make changes to the medications prescribed for several patients, endangering their welfare.

### 4.1.3 Audit Trails Useless

Audit trails keep track of who did what to which records at what time. All auditing systems require solid identification and authentication; without knowing the identity of the human being using the workstation or terminal, audit trails are useless. However, in the circumstances described above, where a session is established by the first person to log on and then left throughout the day, all transactions are attributed to the initial log-on, making audit trails useless.

## 4.2 Options for Improving Medical Identification and Authentication (I&A)

In recent years, technical developments have created excitement about alternatives to the usual forms of identification and authentication (often called *I&A* in the security field) used to control access to restricted data.

All I&A depends on one or more of the following characteristics:

- What you know: passwords or pass phrases; private information such as the color of your first love's hair.
- What you are: characteristics of your body; retinal patterns, iris patterns, hand geometry, fingerprints, height-to-weight ratio.
- What you do: dynamics of speech, signatures and typing.

 

- What you have: tokens, keys, passcards; anything unique or nearly unique that is difficult to obtain or counterfeit.

### 4.2.1 Biometrics

Why not dispense with the token altogether? Why not take advantage of the uniqueness of physical characteristics of the human being or of unique patterns of behavior?

Retinal scans, iris scans, fingerprint recognition, and hand-geometry readers and signature dynamics recognition all take at most a few seconds to operate — perhaps 30 seconds in all. Unfortunately, the equipment for reading these biometric attributes costs at least hundreds on up to thousands of dollars per station. Even speech recognition requires specialized equipment and relatively expensive software.

The same problem interferes with effective application of most biometric methods in the medical sphere: they are great for establishing I&A and starting a session, but they don't solve the problem of having the user disappear and another take his or her place at the open session, thus fouling up access controls and trashing the audit trail.

There is, however, a particularly promising biometric technology that has recently been demonstrated at trade shows and implemented in a few situations: facial recognition. Small cameras in enclosures about 6-8" high can be positioned at workstations. When the user simply looks at the mirror, the camera can analyze the face and match special parameters of the face with stored and encrypted data about the authorized user. With such a system, it is unnecessary to do anything other than sitting down at a terminal or workstation in order to gain access to data. It is also impossible to step away from the workspace without having the camera detect the departure and lock down the session until the next user appears.

In the medical context, this system would be ideal; there is no interference with the user — the system appears to know who you are instantly and provide access to just the records for which you are authorized. There is no delay in accessing the information you have a right to see and work with; you cannot leave the terminal unlocked even for a moment; and the audit trails are precise and complete.

The current price of this new technology has dropped to less than $100 per workstation – perhaps within reach at last. In addition, cooperation from medical malpractice insurance companies may help defray the costs of such equipment on the grounds that it could reduce the actuarial risk of malpractice.

### 4.2.2 Tokens

Tokens such as physical keys are familiar to all; however, physical keys are very easy to duplicate. Even those marked DO NOT COPY can be copied at will in any corner store tended by a clerk instead of by a bonded locksmith. Various other kinds of cards, originally more difficult to copy, have been invented and tried over the years: infrared patterns, magnetic stripes, even cards identified by the distribution of elongated particles to create a unique reflected *signature* when bombarded by a radio-frequency emitter. The latter, called *Wiegand cards,* are

 

of particular interest because they can be used with *proximity sensors;* that is, they can be sensed at short distances without physical contact with a reader. Many such cards can be sensed even without removal from wallets or purses.

Passive tokens of this kind usually cost only a few dollars each; the equipment for writing them may cost a thousand dollars or so, and the readers usually cost in less than $100.

In recent years, security specialists have been particularly impressed by cards containing a microprocessor: the *smart cards* so useful in storing patient and other data. Some smart cards serve as password generators; they create a unique encrypted sequence that depends on the particular date and time plus the serial number of the particular card. This encrypted sequence is decrypted by software running on the host computer or network server and allows unique identification of which card is being used to generate the unique sequence. No other card can generate the same sequence at the same time; and the password expires after about a minute or so. Because each password is useless after its one-minute lifespan, even someone seeing or intercepting the password finds it impossible to use for unauthorized entry to the system.

Several companies are offering smart cards in the form of USB tokens which work with all modern computers.

Most of these smart cards cost in the range of a few dollars up into tens of dollars; they usually have a fixed lifespan (due to the combination of a battery and a case that precludes tampering) of a few years. Readers cost around a hundred dollars (or are standard equipment on PCs in the case of USB tokens).

Although all these tokens have advantages over normal physical keys, they all share the same problem from the medical worker's point of view: they either get read once (which means they can be taken away and the session they initiate left unattended) or they have to be placed in some sort of reader while one works — with potentially disastrous results when the worker hurriedly gets up and forgets to remove the token. Ripped clothing, yanked wrists, damaged readers or cards and a spate of blue language usually follow. The most promising technology of this class is proximity cards, either using the Wiegand effect or interactions with a smart card. Even such tokens, however, can be left at the workstation deliberately or by mistake, again causing difficulties of access control and errors in the audit trail.

In May of 2004, I learned of a product that may solve I&A in the medical context. The XyLoc system from Ensure Technologies Inc. < http://ensuretech.com > uses active radio transceivers. One is carried as a badge and the other is attached to each workstation. The system senses the proximity of the badges and supplies the operating system with the identification numbers and distance of each badge within range. One can configure the system to initiate a session when a badge reaches a critical distance from the workstation and to suspend or terminate the session when the badge is taken away. It is even possible to identify a badge that has been taken off and left on the desk because normal users do not remain immobile for very long. The system includes single sign-on software permitting easy access to medical application programs. It also enables users to transfer their sessions automatically from workstation to workstation without having to re-authenticate themselves – a real benefit to medical workers. This system has already been well received in many medical centers and high security applications.

 

### 4.2.3 Hand-held computers

Another device that is not usually considered part of the weaponry of the information security specialist actually could be in the medical context. Hand-held, powerful computers have appeared that are capable of running reduced versions of normal operating environments (e.g., Windows CE) and that are equipped to communicate using infrared beams (at short distances) or cellular or other wireless radio for longer distances. Such devices could easily be uniquely identified (e.g., by inserting a PCMCIA card with a cryptographic module). To serve as a basis for secure access to medical data, however, two criteria would have to be met:

- every single health-care worker needing access to medical information systems would need to be assigned a unique, non-sharable device (or at least a unique PCMCIA card) for purposes of I&A;

- not one such worker could lend their I&A device (the computer or the PCMCIA card) to anyone else.

Such systems might work, but they would depend more on human cooperation than, say, facial recognition systems.

## 4.3 Restricting Access Privileges in a Health-Care Team

Even if we could deal with I&A and get them completely out of the way, another problem faces the modern medical care establishment. Modern practice emphasizes team work and followup, so determining adequate and appropriate restrictions on who can see or modify which records is a difficult balancing act.

## 4.4 Social Psychology Militates Against Restricted Access

Another factor is the academic connection; medical care is closely tied to the academic mind-set. Many hospitals are affiliated with medical schools; many of the staff members, especially doctors, hold academic positions. Even in health maintenance organizations and private clinics, the academic connection is strong. As a result of this fruitful and valued connection, it is possible that the academic distaste for secrecy carries over into the medical environment. Protecting patient confidentiality just doesn't seem like much of a worry.

The sense of collegiality may also contribute to disdain for security. After all, when members of a medical team share crises, joy and pain, weariness and triumph day after day, why would they think of protecting information against unauthorized modifications or accidental damage? The sense of trust naturally extends to trust over handling of patient records.

The unprecedented ease of access to medical records also makes information security difficult to sell. The computerized medical record is still being implemented in much of the medical field, and paper charts have been handled safely for decades without much difficulty; why then should computer-based records cause such a fuss? The main problem with computerized records is that they provide faster and more extensive access to data than any manual system could possibly

 

provide. For example, if paper charts are kept at a nursing station, it may take minutes to locate the records for any given patient; on a computer-based system, lookups are a matter of seconds.

Paper records for patients who have moved out of a ward, for example, are likely to move to archives, where the archivists scrutinize unusual requests for charts; however, when the records are computerized, it may easily happen that records remain active or accessible longer than they used to be.

### 4.5 Changes in Technology are Not Recognized

Computers allow rapid selection of particular groups of patients; e.g., everyone being treated for a particular disease or using a particular medication. Such information may be of competitive value to pharmaceutical and insurance firms; unscrupulous employees of such firms may suborn medical or para-medical staff (e.g., orderlies, cleaners and security guards) to steal this information.

The density of information storage of today's computers generates another threat: that large amounts of information can be copied and stolen with virtually no chance of detection. A single 1.44 MB diskette, for example, can hold the equivalent of a several hundred closely-written pages; a ZIP disk, with 250 MB on a device the same size as a 3.5" diskette, holds thousands of pages. Modern USB flash drives can be purchased at any computer store in capacities ranging into the Gb for no more than a few hundred dollars. A 5 GB DAT cartridge the size of an audiocassette can hold more information than hundreds of volumes of case reports — and fit unnoticed into a shirt pocket or a purse.

In 1980, I worked with 120 MB disk drives capable of holding about the same as an old-style ZIP 100 MB cartridge; the removable magnetic disk packs were a foot high and two feet in diameter (and cost over $1,000). USB and FireWire ports are commonplace today and allow extremely rapid data transfers without having to load special software.

The pace of change in technology has been so great that it seems likely that many of the people in the medical field simply are not aware of their increased vulnerability to data theft and other forms of compromise.

### 4.6 Restrictions are Difficult to Define for Interdisciplinary Medical Care

In general, all the health-care staff in a particular service or ward will have equal access to all patient records, or at least to all records of patients currently under treatment. In a metropolitan hospital I once worked with, the medical informatics committee decided to define the treating team as closely as they could. They were appalled by the explosive reaction of the religious workers in the hospital. The chaplains (ministers, priests and rabbis) were horrified at their exclusion from access to the full medical records of all the people for which they were responsible.

 

### 4.7 Lack of Resources

Finally, the lack of resources experienced by some components of the medical care delivery system conflicts with information security requirements. For example, the difficulties in controlling access to shared terminals and workstations makes hand-held, personal digital assistants with wireless access to encrypted medical data an obvious choice for the medical environment, but few hospitals have moved in that direction, perhaps in part because of the cost — several hundred dollars for each professional in the medical system who needs access to patient data.

## 5 How to Motivate Medical Administrators to Pay Attention to INFOSEC

One of the most difficult challenges in medical information security is convincing upper management to pay attention to the issues described above. The following sections suggest methods of gaining and keeping management support for information security.

### 5.1 Gain the Support of Key Members of Management

In today's corporate culture, the obvious way to present information is in a meeting of several people. Most people assume that meetings are an effective use of time; after all, why repeat the same information separately to several people when you can prepare a slide show and talk once? Unfortunately, this belief is contrary to evidence of social psychology, which emphasizes the disproportionate effectiveness of face-to-face discussion. Spend the time required to engage in meaningful, genuine dialogue with the decision-makers in your organization; show them sound reasons for paying attention to information security. Enlist their support for your point of view — but remember that a major advantage of such one-on-one meetings is that you will learn about upper management's concerns and beliefs. Senior members of the administration may be able to point out sore points to avoid and hot buttons to push when you do come to address a larger meeting.

Find out by discussion with your colleagues which of the senior staff would be most amenable to your request for a hearing on the matter of information security. Approach each of these decision-makers simply and sincerely: tell them you need their help and ask them for their advice and support. Learn from them who else you should approach individually; ask if you should mention their name when contacting others. Build a consensus one person at a time instead of insisting on mass-production techniques.

### 5.2 Present Awareness Seminar to Upper Management

Developing information security policies and procedures necessitates extensive work with all sectors of the organization involved. Such impositions on colleagues' time cannot be undertaken without authorization of the managers involved. The process thus becomes a kind of bootstrap operation, where we have to start with a very small request and generate a minimum of support for the whole project.

A good start in getting upper management's attention is to address a gathering of high-ranking authorities within the organization. If there is a medical informatics committee in the

 

organization, that would be a good place to start; otherwise, one could ask for support from the highest planning committee in the organization.

The first request should be for a modest presentation — perhaps 30 minutes at most. Begin with a few comments on fundamentals of information security; include a few case studies from your own organization if possible or refer to documented cases.

### 5.3 Work with Corporate Legal Counsel & Facilities Security Staff

If possible, involve your allies in your organization to make a solid case to upper management. Plan to include supportive statements (perhaps even the presence of) your corporate legal counsel and your chief of facilities security. These professionals will have to work with you throughout your efforts to improve information security, and it is important to be sure that they are seen as equal partners in the organization-wide efforts. The advent of HIPAA in a sense makes the argument easier than in the past.

### 5.4 Perform a Preliminary Assessment of Information Security

Your request to the upper managers must be to gain their authorization and explicit, written support for you to conduct a preliminary assessment of information security at your site. This effort need not and cannot be extensive, since you have to start small to avoid being crushed; think of yourself as a small, bright, fast-moving mammal in Jurassic Park or the Lost World. Your task is to get information without offending anyone and certainly without alienating such big players as the director of professional services or the head of emergency medicine.

Your preliminary assessment can consist of spending half an hour simply asking managers in the different sectors of your organization to tell you about their concerns about security. Use the Parkerian Hexad as a checklist if you like; it may help stimulate discussion with your colleagues. Remember to include questions about disaster preparedness. In all interviews, do not express dismay or horror at the abysmal levels of information security you may find; this response will not serve to enlist your colleagues' support in future exercises. Your job right now is to find out what's wrong (and what's right), not to fix problems.

If someone requests anonymity grant and respect it. Anonymity is not appropriate in a thorough analysis among professionals, but it can be justified for the first pass because there is not enough time to delve into details.

If you have the time, you can also circulate a questionnaire to colleagues asking them about information security; however, devising a questionnaire that conveys accurate and complete information is a difficult task. In my experience, response rates will be low and the quality of responses will be questionable.

### 5.5 Analyze Preliminary Findings

Analyze the results of your interviews by organizing the comments into categories that make sense in your circumstances. You can use a spreadsheet to write out each substantive remark or expression of feeling (one per line), then assign a provisional category to each line and sort by

 

category. Within each group of sorted categories, you will be able to subdivide the findings further by adding another column for the secondary code. Then sort again using both the major and the minor categories. This simple technique is called Computer-Aided Thematic Analysis™ and I have used it for over a decade.

### 5.6 Find Necessary Expertise for Corporate Information Security Assessment

Before presenting your findings, contact several sources of independent expertise in medical information security. Independent experts can ask questions that insiders may not think of or may be reluctant to ask; their wider experience of information security can help not only identify problems but also propose concrete solutions. However, outsiders should have no axe to grind and no hidden agendas; be sure to get references from clients before accepting anyone as a candidate for this sensitive assignment.

Consulting firms may be able to help, as can colleagues from other medical institutions, especially from institutions similar to yours. Ask them if they know professionals who can help you in an assessment. Determine approximate costs of an assessment. Typically, assessments will require at least one week of on-site interviews, and at least twice that in analysis and report writing. The chronological time span will exceed the time on site and for analysis because not everyone will be available at the same time and because there are likely to be followup questions and interviews to fill in critical sections of the analysis. Expect to pay somewhere in the $50,000 range and up for a professional analysis of a metropolitan hospital. Costs will increase as a function of the complexity of data manipulation and especially if there are many different networks, operating systems and application programs involved.

### 5.7 Report Preliminary Findings

Distribute your preliminary draft findings to the people you interviewed. Ask them for corrections, comments and suggestions for improvements. Incorporate the improvements. Distribute the final version of your preliminary findings at least a week before the meeting where you have arranged to report to upper management. Call the principals a couple of days before the meeting to ask if you can provide any clarifications or additional information (and also to remind them implicitly to read your report).

Present the preliminary findings in a short presentation to upper management. Half an hour and 10 slides should be enough to make the main points. Lay out the budget you need to perform a thorough assessment and describe the options you have found for performing the assessment. Be prepared to make a recommendation of the person or group you would prefer to work with.

### 5.8 Perform Corporate Information Security Assessment

The experts you hire for the security assessment should work closely with at least one person on your staff — the person designated to work full-time on information security (now or in the future). In my opinion, the head of informatics should *not* be the person you choose; there is too great a possibility of conflict of interest if major problems are found during the analysis. You do not want people sabotaging the project (consciously or unconsciously) in order to protect their turf.

 

In each interview, make it clear that the expert is not conducting an external audit; there is no intention of apportioning blame. Be sure that all interview data are sent back to the people involved for verification and correction. Circulate the draft report from your consultant(s) to everyone involved in the process before submitting the final draft to upper management. You have to make this a communal effort or you will generate resistance and hostility instead of interest and cooperation.

Present the assessment report and its detailed recommendations to the people who authorized the study. Ask for authorization to assign a full-time staff person to develop and implement policies and procedures for improving information security in your organization.

# 6 How to Develop and Implement INFOSEC Policies in the Medical Field

Getting from the assessment report to actual improvements is not so easy. Expect to see efforts extending over many months of work and involving all sectors of the organization.

## 6.1 Hire Professional Staff for INFOSEC or Train Your Own

If you have staff on board who already have experience in information security, all the better. Otherwise, you may have to hire someone with experience or train a suitable volunteer from your own staff — usually someone from the informatics group. Ideally, this person should not report to the head of informatics but rather to a management group dedicated to information security.

## 6.2 Gather input from Information Protection Working Group

Each organization should gather committed, able people who care about safeguarding the interest of patients and of the organization as a whole and form an Information Protection Working Group. Avoid the use of the word “security” in such a title; it creates resistance. The Group should expect to meet every couple of weeks or so; perhaps more often at the beginning of the process.

## 6.3 Communicate with Colleagues to Share Insights and Policies

There are surely others who have similar situations to face; work with these colleagues to share policies and procedures, to discuss case studies, and even to have joint meetings now and then. Use the experience of vendors and consultants in your work.

## 6.4 Integrate INFOSEC with Disaster Prevention, Mitigation and Recovery Planning

Much of the analysis and problem solving for both security and disaster recovery planning is in common. Take advantage of this parallelism and leverage interest in each sphere to help the other prong of your strategy.

 

### 6.5 Use Social Psychology to Change Attitudes and Improve Compliance

Many commentators have observed that information security, like quality, is more a matter of corporate culture than of technique. People have to learn — and want to learn — new ways of working with information in order to improve security. Security cannot be an add-on or a trick.

The findings of social psychology have much to teach us about social cognition (how people form judgements about issues) and effective methods of enlisting support for a position.

### 6.6 Develop Security Awareness Programs

If security is relegated to a couple of pages of dry text to be signed upon joining your organization, or if security manuals pile up, forgotten, in dusty corners of people's offices, your information will never be secure.

Successful information security policies and procedures have to be integrated into whole-organization efforts to keep security in the foreground as a necessary consideration in everything people do. Posters, campaigns, contests, prizes — all can play a role in helping to improve security awareness.

### 6.7 Monitor Compliance with Security Policies

Finally, any set of policies and procedures will fall into disuse if management show no interest in supporting them. Monitor compliance with your security policies; praise and reward those who protect information and improve policies; correct those who endanger patient health and other interests by disregarding security. Make the rewards and the punishments quick and just, but be sure the people enforcing these policies are not authoritarian bullies. Ham-fisted enforcement will alienate the very people on whom you depend to keep your organization and your patients safe.

## 7 For Further Reading

Bosworth, S. & M. E. Kabay (2002), eds. *Computer Security Handbook, 4th Edition.* Wiley (New York). ISBN 0-471-41258-9. 1184 pp. Index.

Dick, R. S., E. B. Steen, & D. E. Detmer (1996), eds. *The Computer-Based Patient Record: An Essential Technology for Health Care, Revised Edition*. National Academy Press (Washington, DC). ISBN 0-309-05532-6. 270 pp. Index.

Donaldson, M. S. & K. N. Lohr (1994), eds. *Health Data in the Information Age: Use, Disclosure, and Privacy*. Committee on Regional Health Data Networks, Institute of Medicine. National Academy Press (Washington, DC). ISBN 0-309-04995-4. 272 pp. Index.

Field, M. J. (1996), ed. *Telemedicine: A Guide to Assessing Telecommunications for Health Care.* Committee on Evaluating Clinical Applications of Telemedicine, Institute of Medicine. National Academy Press (Washington, DC). ISBN 0-309-05531-8. 288 pp. Index

JCAHO (1996). *An Introduction to Management of Information Standards for Health Care Organizations* Order Code: KF-100U. See JCAHO publications catalog on the World Wide Web <http://www.jcaho.org/pubedmul/publicat/pubcat/cat_frm.htm>.

 

OTA (1993). *Protecting Privacy in Computerized Medical Information*. U.S. Congress Office of Technology Assessment. U.S. Government Printing Office #OTA-TCT-576 (Washington, DC). ISBN 0-16-042074-1. viii + 157. Index.

 