



Solving Legal and Business Problems of Health Care Providers for Over 30 Years

140 West Germantown Pike, Suite 200  
Plymouth Meeting, PA 19462-1421

[www.healthcaregroup.com](http://www.healthcaregroup.com)

1.800.473.0032

## Is Your Practice Secure Against Electronic Data Risks?

While a godsend to productivity, the growing prevalence of electronic record keeping is increasing the amount of related risks to which medical practices are exposed. As a result, efforts are intensifying to prevent these security violations.

Besides health care specific risks, such as stolen medical records and liability for medical information provided over a website, medical practices are also subject to general electronic hazards, such as computer viruses, like the infamous "Love Bug" virus. However, in a health care situation, the consequences, financial and otherwise, can be much more harsh.

Medical practices must assess their exposure to electronic tampering, and at the same time they also need to evaluate their risk coverage for these situations. No matter how well you think you are protected, it is impossible to foresee every scenario that could happen. Even with regular audits and written procedures, there is still residual risk, such as disgruntled employees, new viruses, and more knowledgeable hackers. In addition, older insurance policies may not cover electronic risks. Risk management will soon have to include insurance that covers data tampering and electronic threats. The security of your medical practice is only as good as the weakest link in the entire system. If you submit information electronically to an entity that doesn't have a sufficient security policy, you have in effect negated all of your protective measures.

Technology to support internal access policies includes passwords and authentication measures. One such method is *biometrics*, in which the user is required to present identification to gain access, such as a retinal scan, voice recognition, or fingerprint recognition.

External methods of protection include encryption technologies, digital signatures, and firewalls. A firewall is a combination of hardware and software components used to protect an internal network from potential security breaches by way of the Internet. However, even the best firewalls can be breached by a determined hacker, thus a firewall is usually the first line of defense against outside intrusion.

The Health Insurance Portability and Accountability Act (HIPAA) isn't the only issue for medical practices, although it has put protective measures more on the forefront than before. This piece of legislation requires your practice to protect and secure clinical information. In addition, you must maintain adequate computer systems and management controls over the use of your system.

Security concerns are growing more and more extreme. Remember that websites and e-mails are not guaranteed to be secure. It has been proven that you don't need to be a computer expert to hack into a website. Upset employees with the right authorization can steal sensitive electronic information. In fact, most breaches of security are the result of personnel problems, and not inadequate technology. It is important to make sure your employees are aware of the punishments for improper access and unauthorized use of patient information.

Medical practice managers and administrators need to be aware of the risks associated with electronic tampering. However, it is sometimes difficult to wake up and take action until it is too late and a breach of security has occurred. Situations involving security infringements are typically more serious for smaller practices that might not have firewalls. However, all sizes of practices can suffer a damaged reputation from such an incident. No practice wants to have the stigma of not being careful with confidential patient information.

A practice wanting to assess their security risks should first take a look at what is going on around the office, such as employees sharing passwords or taping them to the computer monitor. Once you have an idea of what security blunders are occurring, you can establish protocols, even for such basic things as using computer virus prevention software. Data security begins by educating your staff

members who have computer access to confidential data and monitoring and enforcing clearly written security guidelines. Does your practice have a policy regarding the sharing of passwords? What about an e-mail policy? Define the staff members that absolutely need access to clinical information, and give authorization only to those individuals.

A good procedure to have in place is to deactivate system passwords immediately after an employee is terminated. Computer users unaware of the seriousness of data tampering tend to choose easy-to-guess passwords. Make sure employees select less obvious passwords.

Making sure your medical practice is secure against electronic data interference and theft is a technology matter, as well as a risk management concern. Patients rank privacy high on satisfaction surveys, and they will be unlikely to give out confidential information if they are concerned about where the data will end up, possibly affecting the outcome of their treatment. It is crucial for medical practices to protect the confidentiality of medical records, and at the same time make sure that the information isn't so secure that health care providers don't have the access to information when they most need it.

## **HEALTHCARE DATA RISKS**

- Patient information being displayed on an unattended monitor
- Unauthorized computer access by terminated employee
- Sharing or writing down of passwords
- Computer viruses
- Theft or misuse of hand-held devices carrying patient information
- Internal data that becomes accessible to Internet users outside the practice
- Inappropriate sharing or forwarding of information via e-mail

## **RISK REDUCING STRATEGIES**

- Firewalls
- Encryption of data sent over Internet
- Situate workstations so unauthorized people cannot see the information displayed
- Frequent password changes
- Current antivirus software
- Compliance with HIPAA regulations
- Require staff to sign confidentiality contracts
- Automatic workstation timeouts after a few minutes of nonuse

---

*A version of this article was submitted for publication. It was reviewed and updated in 2006. Permission is hereby granted for the reprinting and use of this article provided that such distribution is free, and provided that the source and ownership of this material is acknowledged to be The Health Care Group, Inc.®. This article can be found online at [www.healthcaregroup.com](http://www.healthcaregroup.com).*