How to Protect Your Practice From a Digital Disaster: Create an E-Mail Policy

Mark Roozen, DVM, MBA

Author's address: PO Box 485, Millersburg, KY 40348; e-mail: mbavet8@gmail.com. © 2013 AAEP.

1. Introduction

Computers are here to stay. That seems pretty obvious, with our growing reliance on the various digital and electronic devices that are required to do business. Along with the computers, we have also become Internet-dependent. Because the Internet is firmly planted as an integral part of our business process, digital communication has also become a major part of practice.

Currently, the primary business form of digital communication is still e-mail. This may change, but this use of the computer offers employees an efficient way to exchange information. The problem is that computers and the efficient transfer of data can get the unsuspecting business owner in trouble. Employees can send out vital secrets, private patient information, or harassing messages to clients or to the public. They can also receive or download a whole host of problems in the form of malware, pornography, or illegal software.

Do your employees understand the use and potential abuse of the business computer? Can you search your business computers for potentially dangerous or libel e-mails without creating legal problems? Do you have an e-mail policy in place?

2. Discussion

An e-mail policy is critical in today's business environment of increased exchange of digital information. A clear and informative policy will not only offer you some protection but it will give your employees a chance to understand the limits and cautions required when they use business computers to transmit e-mails.

There are five basic policies to consider for your e-mail protocol. These include, but are not limited to, computer ownership, e-mail ownership, e-mail retention, e-mail privacy, and proper e-mail content (netiquette). There are other components that can be added for a more detailed and complete policy. These might include protocols for cell phone use, spam, downloads, networking, texting, and online security; however, if you have no policy in place, at least start with the basic five.

The first component of your e-mail policy is to make ownership and use of your computer system very clear. The point here is to make sure your staff is well aware that all components of your digital system are company property, including the software and the data. These electronics are for the primary use of doing business. If your company allows personal use of the computer system, then you should also establish clear guidelines for non-business use.

Following the chain of ownership, the next policy establishes who actually owns the e-mails. The basic premise is that each and every e-mail generated from within the business e-mail system is the prop-
property of the business. If the e-mail system is based on a server within the business, most employees can understand that ownership. When the business e-mail system is based on a remote server such as Yahoo, Gmail, or AOL, some employees have difficulty understanding that the e-mails are the property of the business. This does not include the private e-mail accounts of your employees who reside on these remote servers, but it does include the individual accounts that are within your business e-mail system such as Outlook.

Clarifying the ownership status of the e-mails lends itself to the next component of your policy that addresses the expectation of e-mail privacy. Protection of your business demands the ability to access relevant and critical information, even if it is contained within an e-mail. This means that your employees should not expect their e-mails to be private. Of course, this does not mean that you are going to monitor their business e-mail accounts every day, but they should be aware that inspection is an option to the business.

Being able to review the e-mails of any employee in the business leads into the next policy that establishes the right of the business to purge the e-mail system. We all know how the numbers of e-mails have blossomed over the years. The sheer number can tax the memory volume of most storage devices. You can choose to buy more and more memory, or you can choose a more effective method and purge all e-mails on a regular basis. The time frame that seems to be the most effective for veterinary practices is 90 days.

This means that any relevant information that remains in the e-mail system will be deleted. Consequently, there should be an e-mail retention policy that offers clear guidelines for what information should be saved. E-mails that contain information related to medical records should be moved to the proper patient record. If the e-mail contains relevant business information, then the e-mail should be printed or digitally stored in the proper business folder.

However, be cautious. If there is a pending legal matter that encompasses digital communication, then the purging process must be suspended.

The final component to incorporate into your policy is a guideline for e-mail content. When business e-mails are sent, they represent the practice. This includes the practice culture and attitude. Having guidelines for how the e-mail is written is critical to maintaining your professional image.

Imagine that one of your clients is considering a sophisticated and expensive procedure. Then they get an e-mail from your office that is full of grammatical or spelling errors. This has the same image as performing a beautiful arthroscopic procedure on a knee only to send the horse home with a leg bandage that is sloppy and dirty. Established basic e-mail content protocols might prevent your best client from receiving a message that is all capital letters, the digital equivalent to screaming. Offering your employees e-mail content guidelines will help maintain professionalism.

3. Summary
In today’s digital business environment, it is crucial to have clear and concise guidelines that inform your employees and protect your business. Once the e-mail protocols are established, make sure to incorporate them into your practice. The best way to ensure awareness is to insert the completed policy right into the employee handbook. A stand-alone policy document is also possible, but, in either situation, the contents should be reviewed with the staff and their exposure to the policy confirmed with a signature.