Cyber Security and the Dental Office (Part I):
Protecting Your Office Computer Network

Scott Aurnou, CIPP/US, CIPT
Continuing Education Units: 2 hours


Disclaimer: Participants must always be aware of the hazards of using limited knowledge in integrating new techniques or procedures into their practice. Only sound evidence-based dentistry should be used in patient therapy.

Note to State of Florida dental professionals: This course does not meet the 3 credit hour minimum for Practice Management courses; therefore, it is only being offered for informational purposes in Florida.

This continuing education course will provide dental professionals and office staff a basic understanding of the potential cyber threats facing a modern dental office, as well as the fundamental steps needed to protect computers, mobile devices, office networks, and the practice and patient data they contain.

Please note this is Part I of a two-part series. To gain the full benefit of the concepts covered in this course, be sure to read Part II (Be Prepared: Hacker Tricks and Security Emergencies).

Conflict of Interest Disclosure Statement
• Mr. Aurnou reports no conflicts of interest associated with this course.

ADA CERP
The Procter & Gamble Company is an ADA CERP Recognized Provider.

ADA CERP is a service of the American Dental Association to assist dental professionals in identifying quality providers of continuing dental education. ADA CERP does not approve or endorse individual courses or instructors, nor does it imply acceptance of credit hours by boards of dentistry.

Concerns or complaints about a CE provider may be directed to the provider or to ADA CERP at: http://www.ada.org/cep
Course Contents

Introduction

Relevant Legal Standards

Pertinent Tech Basics – What You Need to Know

Protecting Your Laptop and Desktop Computers

• Protect Your Computer
• Physical Security
• Don’t Forget Email
• Disposal

Safeguarding Mobile Devices

Protecting Your Office Network

Conclusion

Course Test

References

About the Author

Introduction

Modern dental offices are run electronically. While this offers many advantages for speed and efficiency when dealing with patient records and internal office data, it also exposes those offices – and their patients – to new dangers. Whether it's due to a simple mistake or cyber thieves, exposed patient data can lead to heavy fines, public embarrassment, lost business and substantial remediation costs. Recent studies have found that data breach costs for healthcare providers can run as high as $363 per record lost. While there is no way to make an organization completely impervious to any electronic threat, smart cyber security measures can help you protect your patients and your practice.

Relevant Legal Standards

Much of the heightened level of risk facing a modern dental practice pertains to their patients’ Protected Health Information (PHI). PHI relates to the past, present, or future physical or mental health or condition of a patient and provides a reasonable basis to believe that it can be used to identify the patient. This includes healthcare/dental information containing any of a number of patient identifiers including name, date of birth, Social Security number, telephone number, medical record number or ZIP code. Even a patient’s name and reason for an appointment can be enough to qualify as PHI.

Cyber criminals pay far more for PHI than credit card information or Social Security numbers alone. Unlike a credit card, patients can’t simply cancel and replace their life history. PHI is just the sort of information cyber criminals need to impersonate someone effectively when
attempting to open fake credit card accounts or submit fraudulent tax returns. Patient information can also be used to create fake billing for Medicare or Medicaid or in conjunction with an unethical medical provider to write prescriptions for narcotics that are subsequently sold on the street at a very high profit margin.\footnote{5}

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) affects healthcare providers, healthcare plans and various types of vendors working with PHI. Dental offices using computers, electronic data storage, the Internet, etc. are considered “covered entities” and subject to HIPAA’s requirements. “Business associates” are also subject to HIPAA. They are non-employees that create, receive, maintain or transmit PHI. This includes vendors, consultants and sub-contractors of either who have access to patient information.

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) was intended to stimulate use of electronic health and dental records with financial incentives for providers. It effectively strengthened HIPAA by adding direct accountability for business associates and enhancing its enforcement provisions. In addition, The Department of Health and Human Services (HHS)’ Office for Civil Rights (OCR) was placed in charge of enforcing HIPAA’s Privacy and Security Rules.

The HIPAA Omnibus Final Rule was enacted in early 2013. It effectively codified HITECH rules regarding security, privacy and enforcement into HIPAA directly. This included breach notification requirements, direct liability for business associates and increased fines. The Omnibus Final Rule also removed earlier statutory language requiring a “significant risk of harm” of data loss and makes any use or disclosure of PHI not in accordance with HIPAA a reportable breach.

HIPAA has three primary Rules:

**Privacy Rule:** each covered entity and business associate subject to HIPAA has a duty to prevent unauthorized access to patient files. This relates to electronic, paper and even spoken information regarding patients.\footnote{6}

**Security Rule:** relates to electronic patient files. Covered entities (including dental offices) must take steps to prevent unauthorized access to electronic PHI. The Security Rule has administrative, physical and technical safeguards focusing on steps to improve an organization’s security practices.\footnote{7}

**Breach Notification Rule:** requires covered entities and business associates to provide notice when a data breach involving unsecured PHI has occurred. Proof of actual data theft is not required. HHS defines a data breach as an impermissible use or disclosure of PHI, unless there is a low probability the data has been compromised. There is also a publication requirement mandating a press release to the local media for any breach over 500 patient records. And, as if that’s not bad enough, knowingly failing to report a breach in excess of 500 PHI records to HHS within 60 days can actually result in jail time. But it’s not all bad news: data that is encrypted is considered secured and does not trigger the Breach Notification Rule.\footnote{8}

Individual state laws may also apply, as there are data breach notification laws in 47 states, as well.\footnote{9} A number of law firms practicing in this area have charts available online that summarize the provisions of the various state laws.\footnote{10}

A dental practice can come into OCR’s orbit through a random audit or as a result of a complaint left on the HHS website (which OCR is required to investigate).\footnote{11} If that happens, you need to be ready.

In a dental office setting, there are a few points to focus upon initially. For starters, every dental practice should have a written HIPAA compliance policy clarifying everyone’s role in keeping the office HIPAA compliant and protecting PHI.

HIPAA also requires someone in your office to be responsible for compliance with the Privacy and Security Rules. In a larger organization, this is typically a designated privacy officer. In a smaller office, the office manager or one of the dentists may take on the privacy responsibility.

Staff training is critical. Employee education can save your office from avoidable HIPAA violations.
Your privacy officer should organize regular trainings to clarify everyone’s role in keeping the office compliant. Be sure to document these trainings and have everyone sign a written statement that they have completed their HIPAA training. If an audit letter does arrive, documenting your compliance actions shows them that you’re taking risk seriously and makes the audit process easier.

Be sure to use detailed written business associate agreements with any organization that handles paper or electronic PHI. This will clarify how your vendors, consultants, etc. will handle PHI, which (if any) subcontractors will have access to PHI and what measures will be taken to secure it. This is a critical step. The Ponemon Institute’s Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, published in 2015, found 59% of business associates had suffered a data breach in the prior two years.

Any organization subject to HIPAA must perform thorough and accurate Security Risk Assessments to evaluate potential risk and vulnerabilities to PHI. A corresponding Risk Management Plan is used to address the issues identified in the Security Risk Assessment. Keep in mind this is an ongoing process that must be performed regularly and documented. HHS offers helpful information and a Security Risk Assessment Tool to assist a covered entity or business associate in achieving HIPAA compliance.

On a somewhat related note, if your office accepts credit cards for payment, it will also be required to comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is administered by the Payment Card Industry Security Standards Council (PCI SSC), which was established in 2006 by the major card brands in America and Japan (including American Express, Discover, MasterCard and Visa). The purpose of PCI DSS is to set minimum security standards that organizations must maintain in order to protect card holder data.

Resources
In addition to information available via HHS, there are a number of resources available for additional assistance regarding information security standards, practices and emerging risks.

The United States Computer Emergency Readiness Team (US-CERT) – which is part of the Department of Homeland Security – offers a number of security-related resources, with sections for technical and not-so-technical people. US-CERT’s offerings include explanations of a number of common issues, as well as regular vulnerability and threat alerts.

The National Institute of Standards and Technology (NIST) works to develop cyber security standards across a number of fields, including the standards used as reference for HIPAA compliance. NIST’s Computer Security Resource Center (CSRC) offers a host of security tools, guidelines and other resources, including the Special Publication (SP) 800 series covering a wide range of security topics. One of these is a detailed guide to implementing the Security Rule.

In addition, there are a number of commercial alternatives tailored to the needs of dental and healthcare practices, including the Revised ADA Practical Guide to HIPAA Compliance: Privacy and Security Kit and HITRUST’s Common Security Framework. Well-versed security professionals are a good alternative, as many specialize in HIPAA compliance.

Pertinent Tech Basics – What You Need to Know
Using computers and mobile devices largely concerns storing, retrieving and transferring information more efficiently. Two basic ways to store and access information is via print (like a newspaper, book, or a patient’s written chart or x-ray film) or electronically (reading that same newspaper or book on the Web or a Kindle, storing the chart or x-ray as a file on your office’s computer network, etc.). These are sometimes referred to as static media or digital/electronic media, respectively. Unlike static media, digital/electronic media requires power to access and read, though it’s also easier to search, store and transfer and, of course, it’s always possible to print an electronic record to generate a paper copy.

With dental offices increasingly keeping patient information as electronic dental records (EDRs) – rather than using file cabinets stuffed to the gills with paper – this begs the question: how is electronic data actually stored? At its most
basic level, all electronic data is reduced to seemingly endless lines of 1s and 0s called binary code. Each individual 1 or 0 is referred to as a “bit.” The smallest number of bits that can be read electronically is eight (i.e., 01001010). This is referred to as a “byte” and each one holds only a tiny amount of information. It varies a bit depending on the program using it, though a byte might hold a number, a letter, or perhaps a small word or two. Naturally, bytes are grouped together for data storage and various computer programs. About a thousand (it’s actually 1,024) bytes is called a kilobyte. About a thousand kilobytes is called a megabyte and about a thousand megabytes is referred to as a gigabyte. In case you’re curious:

A kilobyte = 1,024 bytes
A megabyte = 1,048,576 bytes
A gigabyte = 1,073,741,824 bytes

The amount of files a gigabyte of storage can hold will vary a bit, depending on the type of file being stored and perhaps its video, audio or print quality, but a conservative figure sometimes given is that a gigabyte of storage can hold approximately 75,000 pages of text. That means a computer with a 200-gigabyte storage capacity – relatively small by today’s standards – can contain about 15 million pages of data.

This data can be stored in three basic ways:
1. Magnetic storage
2. Optical discs
3. Solid State Drive (“SSD”), aka “Flash” storage

Magnetic storage is commonly used on the hard disc drives found on most computers. Information is stored using positive and negative magnetic charges to correspond with the 1s and 0s noted above. Optical discs like CDs and DVDs store information as binary code that can be read by an optical sensor in a disc drive. Likewise, flash/SSD technology – commonly found in smartphones, USB drives and some laptops – stores that same information electronically. Each system has different characteristics, but they can all communicate with each other since they all store the underlying information they hold as binary code. As a result, electronic information can be transferred easily between computers, smartphones, tablets, USB (aka “thumb” or “stick”) drives and other electronic devices. Of course, without appropriate safeguards in place, this easy data transferability can also lead to data theft...

One way to protect data is to encrypt it. Encryption is the use of an algorithm to scramble normal data into an indiscernible mess of letters, numbers and symbols (referred to as “ciphertext”). An encryption key (essentially a long string of characters) is used to scramble the text, pictures, videos, etc. into the ciphertext. Depending on how the encryption is set up, either the same key (symmetrical encryption) or a different key (asymmetrical encryption) is used to decrypt the data back into its original state (called “plaintext”). Under HIPAA, encrypted data is considered “secured.” As a practical matter, this means a theft of encrypted data does not have to be reported as a data breach (unless the corresponding key is stolen, as well).

The laptop and desktop computers in your office will generally be connected to each other as part of your office’s computer network. Although a network can be designed a number of different ways, a typical configuration could be what is referred to as a “client-server model.” In that sort of set-up, more powerful computers called servers perform centralized functions for your office (email, data storage, etc.), and the individual desktop and laptop computers connected to the network – referred to as “clients” – access the information or functions they need through the servers. That way, for example, every single computer in your office doesn’t have to store every last bit of patient data if there’s a database server with that information that can be accessed as needed from the other computers in the network. Your office network should include all of the computers and devices intended to have access to your office’s data. Each individual computer and device connected to the network is referred to as an “endpoint.”

The device that connects your office (or home) computer network to the Internet is called a router. The Internet itself is effectively the world’s largest computer network. Its vast, decentralized structure allows for the transfer of data across the globe. The World Wide Web is part of the Internet (they’re not actually the same thing) that acts as a virtual network of websites connected via hyperlinks (or simply “links”). Although we see
them as names like www.dentalcare.com, websites have corresponding numerical addresses on the Internet. These are called Internet Protocol – or IP – addresses. It’s somewhat like a street address referring to the same thing as the building at that address in the way that “1600 Pennsylvania Ave.” refers to the same place as “The White House.” In case you’re curious, dentalcare.com’s IP address is 137.177.81.8.

Another thing to consider before we look at specific threats to computers, mobile devices, etc. is the effect of deleting data. That’s because hitting “delete” doesn’t do what you might think it does. Simply put, the data you try to delete is often still on your computers and can be stolen.

Data itself can be divided into three different types:
1. **Active data** is comprised of programs and files visible when you turn on your computer, be it on the desktop itself or in any file folder.
2. **Archival data** is similar to active data, but it’s stored somewhere else, such as on an external backup drive or in “the cloud.”
3. **Latent data** is information on your computer (or network) that’s not visible to you. This can include “temporary” files created when a document is accessed or printed. It also includes “deleted” files.

To understand what happens when a file is deleted, it helps to know a little bit about what happens when a file is created. When a file is first created, it exists as one of the temporary files mentioned above. Once it is saved, an entry corresponding to the file is made in the computer’s “Master File Table.” A Master File Table (or “File Allocation Table” on an older machine) is essentially a computer’s table of contents, allowing the files listed in it to be readily found as active data. When a file is deleted, what is actually removed is the entry in the Master File Table. The actual file isn’t deleted. The computer just puts a little marker next to it to let it know that it can use that space if needed. As a result, even though you can no longer see it, this type of data stays on a computer until it is actually overwritten (i.e., new data is stored in the same place on the drive where the data was residing).

A good analogy to the actual effect of deleting a file might be tearing off the index and table of contents from a large book, but leaving all of the pages intact. It may not quite be as easily accessible, but the information is still there. If a hacker gets a hold of a computer with this sort of information, he or she will most likely be able to reconstruct it. Needless to say, we will discuss proper disposal of data later in this course.
Protecting Your Laptop and Desktop Computers

Desktop and laptop computers can be attacked from a number of angles (or “threat vectors” in security parlance) that can lead to a data breach, an attacker taking over your computer or encrypting your own files from you, or even an intruder gaining access to your office’s bank accounts. Primary threats include malware (short for “malicious software”), “social engineering” attacks, loss and theft. We’ll cover social engineering attacks in Part II of this course. In the meantime...

It is not at all uncommon for your computer to be attacked electronically as a result of clicking on a link to a website infected with malware (often referred to as a “drive by download”). These sites can be encountered anywhere on the Internet, including web searches and social media websites, as well as in the links found in the emails, instant messages or texts you receive. Individual files can also be infected with malware, which will attack your computer as soon as you open or download them. You can run across these infected files as email attachments or nearly any kind of download from the Internet (audio files, games, videos, etc.), it can happen though USB transfer too, if malicious or infected files are on a thumb drive that’s connected to your computer.

Malware comes in a variety of forms, including viruses, worms and Trojans. A virus is essentially a program that’s piggybacked onto another program or a file. When the underlying file or program is opened (or run), the virus starts to work. This also means a virus is effectively inert until someone opens/runs its host file or program. A worm is a self-replicating standalone program that spreads from system to system. This is often done via email. If you’ve ever seen (or experienced) one or more strange emails coming from a friend, family member or colleague’s correct email address, that may well have been a worm trying to spread itself by sending messages with infected links or attachments to people in their contact list. Once the recipient clicks on the link or opens the attachment, the worm can spread to the new system

Trojans make up the majority of current malware. "Trojan" is short for Trojan horse. It’s a hidden program that – like the Trojan horse of Greek legend – isn’t what it appears to be. Among other places, Trojans can be lurking on infected websites or hidden in software downloads, email attachments, and mobile apps. They can hide inside nearly any type of file (audio, video, office documents, pictures, etc.) and will often be disguised as something fun, interesting or important, to tempt you to click on them. While they may seem innocuous, they’re always bad. How bad? In effect, they come in all shapes and sizes and can do just about anything to your computer. This includes recording your keystrokes, spying on you with your computer’s camera and microphone, stealing personal info and business data and often installing a “backdoor” to allow cybercriminals to take control of your computer remotely. Many Trojans can also elude or even disable anti-virus software and other security measures.
A "botnet" is a group of computers that have been successfully co-opted via malware that forces them to be remotely controlled through the Internet. Botnets can be huge, with some controlling tens or even hundreds of thousands of unwitting victims. These compromised computers can be used for a number of purposes, including sending spam and disabling targeted websites with a flood of fake web traffic. This is called a distributed denial of service (DDoS) attack.

Unlike depictions of electronic attacks on television and in many movies, there is generally no alarm or warning of any kind when a computer is attacked or a network is breached.

Fake antivirus malware (aka "scareware") is actually a type of attack that plays on the idea there's supposed to be a warning sign. It will appear as an unexpected pop-up window claiming your computer has been infected by malware, with an offer to fix the problem if you just "click here." The pop-ups are always fake. If you see one, don't click on it (the pop-up itself is typically an infected link that will attack your computer).

Protecting Your Laptop and Desktop Computers

Protect Your Computer

What steps can you take to protect yourself? Here are a few:

1. First and foremost, keep your software up-to-date. Nearly all malware attacks target flaws in software that have already been fixed by the developer via software updates (also known as "patches"). If you have downloaded and installed those updates, the vast majority of attacks against your computer will fail. Many programs can be set to update automatically and it's always a good idea to take advantage of that. Another great way to ensure your computer stays up-to-date is to use software that automatically updates third-party programs (i.e., from a developer other than Microsoft or Apple). Secunia's Personal Software Inspector\(^22\) is an excellent choice for Windows-based computers and AppFresh\(^23\) can be used to keep software up-to-date on a Mac.

2. Use a non-administrative account. Computers come with a primary user account featuring "administrative privileges." Those privileges allow full access to the computer, including the ability to download, modify and delete programs. While you need that to add, change or remove any software on your computer, you don't need it to use the computer on a daily basis or to browse the Web. If an attacker is able to gain access to that administrative account, he or she will be able to cause far more damage to your system. To keep this from happening, set up a user account with non-administrative access for day-to-day use. Setting up these accounts isn't difficult, though it varies from operating system to operating system.

3. Remove any unnecessary applications and services from your computer. All software has flaws and attackers can use those flaws as a means to get into a system. If the programs aren't there in the first place, hackers can't exploit them to attack you.

4. Replace any software that is no longer supported by its developer. Using out-of-date software leaves you completely exposed. Since the software is "out of support," the developer won't take any steps to fix any problems that are discovered (as it would if the software is still being supported). As a result, any weakness is a permanent one and attackers can use it against you at will. Needless to say, that's a pretty serious problem. It also violates the HIPAA Security Rule.\(^7\) A well-known example of this is the Windows XP operating system. Microsoft stopped supporting it in April 2014. If your office is still using it (or any other out-of-support software), it's well past time for an upgrade.

5. Use basic security software. While antivirus software won't catch everything, it's far better to have it than not. Whether you use a Windows-based computer\(^24\) or a Mac,\(^25\) there are a number of good options available. You should also enable the firewall included in the computer's operating system. Firewalls serve to filter incoming electronic traffic (usually based on its source and destination) and should be used whenever they're available.

Physical Security

While recent studies have found a marked increase in technological attacks against healthcare providers,\(^4,26\) the danger presented by the physical loss or theft of devices with PHI on them has been pronounced for years. A 2014 study of
data breach information found on HHS’ Wall of Shame noted 68% of all healthcare industry breaches since 2010 came about as a direct result of lost or stolen devices. While malware attacks have definitely been on the upswing, only 23% of the breaches in that study took place as a result of the electronic theft of data from a compromised computer network. Statistically speaking, your practice can get robbed just as easily as it can be hacked.

Your office itself will be most at risk from an after hours intruder or someone who has effectively smooth-talked their way inside the office... but shouldn't be there. Once he or she is physically inside the office, an intruder can directly access your computer network (and the PHI stored on it) via a server or client computer using just a USB drive. Or, if it's an after hours intrusion, they can simply steal a computer and take the data from it at their leisure. The effect of even one stolen computer can be devastating. One Missouri dental practice was actually bankrupted after a desktop computer (with over 9,000 patient records) was stolen in 2010. While desktop computers typically stay in your office, laptops and other devices can be lost or stolen from just about anywhere. Leaving your laptop (or any mobile device) unattended even for a few minutes in your car, on public transit or at a coffee shop, etc. is highly unwise. One example of what can happen next (among too many to count) involves a Massachusetts provider hit with $1.5 million HIPAA fine due to the theft of a single laptop computer. Another one involves the former head of Britain's MI5 intelligence agency, whose laptop was stolen at Heathrow Airport in 2012. It really can happen to anyone.

What can you do to minimize this risk? Here are a few steps that can help:

1. **Prevent potential attackers from being able to physically access the computers in your office.** Whenever your office is closed, all entrances should be locked and computers should be turned off. Your office’s server (or servers) should be kept in a locked room.

2. **Prevent them from being able to access the computer electronically.** A password-protected screen-lock should be enabled on each computer in the office, with an engagement time of ten minutes or less (preferably less). That way, an intruder encountering a computer that’s still turned on won’t be able to simply start using it. Speaking of… passwords, user names and/or account numbers shouldn’t be written down anywhere obvious (on post-its, under the keyboard, in the top right-hand desk drawer, etc.). A thief will always look there.

3. **Use encryption to protect the data itself.** If a thief has access to a computer that’s only password-protected, it’s fairly easy to access the data stored on it. Encrypting the data can prevent that. Moreover, under HIPAA and many state data breach laws, encrypted data is considered “secured” and the loss or theft of encrypted data from a laptop or desktop is not viewed as a data breach (so long as the corresponding encryption key hasn’t been taken, as well).

The primary types of encryption used to protect the data on a computer’s hard drive are full disk encryption (FDE) and file-based encryption and they serve different purposes. FDE encrypts all of the data stored on a hard drive, but it's only enabled when a computer is turned off. A decryption key is needed when the computer is turned on. Once the key is entered, all of the data is decrypted and the computer works normally until it's turned off again. This type of encryption is effective when a laptop is lost or stolen… so long as it was turned off at the time. There are a number of full disk encryption products available, as well as built-in versions that can be enabled on Mac (FileVault) and commercial grade Windows (BitLocker) operating systems.

Encryption can also be file-based, encrypting individual folders, files, or even certain parts of files. While this is a slightly more involved process, it's also more secure since it still keeps the data encrypted when the computer is turned on. Even if an attacker gets into the system, the data in question will be gibberish without the decryption key. There are numerous file-based encryption products available from many security vendors.

Physically securing laptops, desktops and other devices with office data and PHI is one of the most productive things you can do to safeguard your practice.
Don't Forget Email
Emails containing PHI and other sensitive data must be protected, as well. By its nature, email is not a terribly secure way to share information. When you send out an email, it goes through your network’s email server on its way to a corresponding email server associated with the recipient’s computer or mobile device. It passes through any number of servers along the way from sender to recipient, like a flat stone skipping along the top of a pond. And if that email isn’t encrypted, anyone with access to any one of those servers can read it. Numerous email encryption options are available.36

Disposal
When the time comes to throw away, give away, sell or otherwise dispose of a computer, you should be sure to permanently erase the data on it. Otherwise, the new owner – or someone who has fished it out of the trash (yes, this actually happens) – will be able to read the PHI, as well as any financial, business or personal data, that was on the hard drive when you stopped using it. Often this will also include data you may have thought was deleted but is actually still on the hard drive. Pressing “delete” doesn’t actually erase a file or program permanently and even a moderately skilled hacker will be able to retrieve it. This begs the question: how do you permanently delete the data you don’t want lingering on the computer once you are ready to dispose of it?

The NIST publication related to data disposal is SP 800-88 rev. 1.37 It details three levels of “media sanitization” – clear, purge and destroy. Data is considered cleared when it’s not readily accessible on the computer or device in question, though someone with digital forensic tools (like that moderately skilled hacker noted above) can still get at it. Purging involves removal of the data to the extent it is “infeasible to recover” using state of the art forensic lab methods and destroying is pretty much what it sounds like. NIST SP 800-88 references a number of destructive methods relating to computer data. Here are a few common ones:

A typical computer hard drive stores electronic information magnetically. Magnetically stored data can be genuinely deleted via overwriting, demagnetization or physical destruction.

Overwriting refers to storing new data in same storage space as – and effectively on top of – the older data being deleted. A helpful analogy could be thinking of the older data like a footprint on a muddy field. If someone steps on it, the new footprint will effectively “overwrite” the old one. A number of programs exist to deliberately overwrite the data on a hard drive with random 1s and 0s (gibberish, in effect), but it’s a time consuming process – as the data is generally overwritten several times – and it might not make the data completely inaccessible. A hacker skilled in computer forensics may still be able to recover some of the data (assuming it’s worth the time and expense to do so). An overwritten drive can be reused.

Demagnetization (often referred to as “degaussing”) involves using a strong magnet to essentially “pull” all of the 1s and 0s in the binary code on the drive in the same direction, making them all 1s or 0s and rendering the underlying data all but unreadable. This is done with a machine called a degausser. Commercial grade degaussers are quite expensive, and their magnets are strong enough to both virtually destroy the data and render the hard drives themselves unusable afterwards. Keep in mind demagnetization only works on magnetic storage devices and magnetic tapes.

Physical destruction is just what it sounds like: the hard drive is dropped into a metal shredder and completely pulverized. Companies that specialize in this sort of destruction will often take the subject drives, document the subsequent chain of custody and may even film them being dropped into the metal shredder. Such an abundance of caution actually isn’t a bad idea. A major hospital in the United Kingdom asked a vendor it had worked with before to take care of disposing approximately a thousand old hard drives, only to have about 250 of them later show up for sale on eBay. The hospital was then hit with a record fine roughly equivalent to half a million dollars.38 Also keep in mind that mere damage is not enough to guarantee the data on a magnetic drive cannot be retrieved later. Computer forensic experts were even able to recover a significant amount of information from damaged drives found in the wreckage of the space shuttle Columbia.39

As outlined above, each of the methods has its advantages and disadvantages. Overwriting
allows the drive to be used again, while physical destruction is the most certain way to be sure the data is permanently destroyed. As an extra precaution, some organizations protect their sensitive data by first demagnetizing and then physically destroying any type of magnetic storage once it’s no longer in use.

Safeguarding Mobile Devices
Not to overstate the obvious, but smartphones and tablets have become commonplace in modern offices. Given their portability, the main threat to these mobile devices is theft (and loss). If a lost or stolen device contains patient data, it can constitute a data breach under HIPAA and state data breach laws. What steps should you take to avoid that?

1. **Encrypt the device.** If it isn’t already enabled, encrypt your device. It’s easy to do and can be found within the device’s Settings app.

2. **Always set a passcode/password.** A passcode is a four digit PIN code required to use the device. Without one, anyone holding your smartphone or tablet can access everything on it by simply turning it on. For extra protection, nearly all devices offer the option to use a longer alphanumeric password instead.

   A number of phones also allow you to use a fingerprint scanner, though hackers found a way around the technology within days of its initial release.

3. **Turn on the auto-lock function.** Right after you set a passcode or password, you should enable the auto-lock function on your device and set it to as short a time period as you’re comfortable with (preferably under five minutes). Aside from saving a bit of battery life, a shorter period makes it that much less likely that someone will stumble upon your phone or tablet while it’s still turned on.

4. **Back up your data.** Backing up the data on your smartphone or tablet is fairly easy and it’s the kind of thing you’ll REALLY wish you’d done if your device gets lost, stolen, or just stops working. Backing up can be done by syncing your device to your computer, a work network or online (i.e., through “the cloud”).

5. **Enable remote wiping on your device.** In case of loss or theft, personal and business data can be protected from prying eyes. A remote wipe performs a factory reset, erasing all data on a smartphone or tablet. If the device has been backed up, the information can be restored on a replacement (or the original, if you get it back). A number of mobile security apps, as well as Apple’s Find My iPhone/iPad app, can be configured to enable remote wiping. On Apple devices running iOS 7 or higher, Find My iPhone includes an “Activation Lock” feature to prevent anyone who finds or steals your device from being able actually using it. Google added a similar feature called “Device Protection” on devices running Android 5.1 or later.

   Many devices can also be set to do an automatic factory reset after a set number of incorrect attempts at guessing your passcode.

6. **Log out.** Always log out of any sensitive online services and accounts when you aren’t using the phone or tablet. Otherwise, if the device is lost or stolen, whoever has it in hand will effectively appear to be you, whether it’s through a social media app… or your bank.

7. **Don’t have any PHI on a mobile device unless you absolutely have to.** If you’ll forgive the oversimplification, a hacker can’t steal information that isn’t there in the first place. Another concern is malware specifically designed for mobile operating systems (particularly for Android devices). A smartphone or tablet can be exposed to mobile malware via an infected website, online ad or app, or through a weblink or attachment to an email or text message. Most of it isn’t designed to break into a network through the infected device and steal network data, but it can still steal data found on the device itself or simply be a nuisance by inundating your phone or tablet with ads and/or significantly slowing it down. A nasty threat called ransomware (which we will discuss in the next section) also exists for mobile devices. With that in mind, what are the protective measures that you should take to safeguard your devices?

8. **Update your software.** Updates to your mobile operating system and any apps on your
smartphone or tablet often include security fixes and should generally be downloaded as soon as they’re available. And yes, there may already be some available when you first take it out of the box. There is a one caveat to this; sometimes software updates can have inadvertent negative effects on older mobile devices. If your device isn’t the current one, it’s a good idea to check online first to see if there are any articles or online discussions regarding problems with that update for your model phone or tablet.

9. **Use mobile security software.** While security apps won’t protect you from everything, they do offer helpful features including device tracking apps and protection against some mobile malware. There are a number of good free and paid mobile security apps for the Android OS.

10. **Don’t jailbreak or root your phone or tablet.** "Jailbreaking" or “rooting” a mobile device refers to overriding the manufacturer’s settings – including disabling the device’s security settings and future updates – to allow it to download and use apps and other features that are normally not enabled on the device (jailbreaking refers to the process as it applies to an Apple iPhone, iPod Touch or iPad and rooting is much the same for a smartphone or tablet running the Android mobile operating system). The vast majority of mobile malware affects these devices since their security systems are badly compromised by the jailbreaking or rooting process, and they should never be connected to a business computer network. Network monitoring software can detect jailbroken and rooted devices and prevent them from connecting to your network.

11. **Check app permissions (and read reviews).** Why would a game need access to your address book? Whenever you download an app, it will request “permissions” which will allow it to use different functions and data on your phone or tablet. It may seem a little tedious, but you really need to check them before saying yes and downloading the app. Apps requesting unnecessary permissions are especially likely with free versions of normally paid apps and apps purchased from third party app stores. Avoiding either isn’t a bad idea. Also read reviews before downloading them – if there are just a few or a lot of bad ones, play it safe and don’t download the app.

12. **Think before you click.** Many tainted websites – including the links in an email or text message – are infected with mobile-specific malware that can be extra tricky to detect, since you can’t hover over the link (to see if it isn’t what it appears to be) with a mobile device. Your best defense against a number of electronic attacks against your mobile device is your common sense. If it doesn’t look quite right or sounds too good to be true, it probably is and you should leave it alone.

**Proper disposal of mobile devices** is somewhat similar to other types of data disposal, though smartphones and tablets use solid state drive/flash data storage, so any magnet-based attempts to erase the data won’t have any effect. What will? Glad you asked – here are two methods:

- A properly executed “factory reset” will electronically reset the device to its original
unused state, removing all data and downloaded applications. It can be found within the device’s Settings app or triggered via remote wiping. If you really want all traces of the information gone, remember to delete synced data, as well.

• As with other types of data, physical destruction will leave no doubt (and no phone afterwards).

If you’re curious for additional detail regarding the proper disposal of mobile data — including what constitutes “clear,” “purge” and “destroy” for each type of device, take a look at NIST SP 800-88.37

Protecting Your Office Network

The primary electronic threats to a dental office network include data breaches, theft of office funds and/or resources and business interruption attacks.

Data breaches can occur as a result of attacks from either inside or outside of your office, or simple human error. External attacks will typically get started as a result of deception, which we will cover in Part II. Once an attacker has gotten into your network and perhaps accessed someone’s account, they will often try to steal login credentials giving them greater and greater access. These attacks will often target the PHI available in your system and sometimes the information needed to access your office’s bank accounts.

In addition to the very real concerns surrounding PHI, intruders inside a network will often try to get financial login details in order to access office accounts and withdraw as much as they can before you or your bank can catch on. A children’s dental practice in Missouri hit with this type of attack was robbed of $205,000 via wire transfers.44

One type of increasingly prevalent financial attack, called a business email compromise, uses a fake email that appears to come from someone you know at one of your vendors and simply “updates” the wire transfer information associated with that vendor. When your office pays the vendor’s legitimate future invoices, the payments will go to the scam artists.45,46 With respect to this particular scam, be sure to confirm any changes in financial information with the vendor by phone (using the number you have on file, not the one in the email) before making any changes.

Business interruption attacks are designed to make it impossible to access data and/or block you or your patients from using some or all of your system’s resources. The main types of business interruption attacks are a distributed denial of service attack (DDoS) and ransomware. A DDoS attack uses hordes of compromised computers across the Internet to overwhelm your website or other parts of your system with so much electronic traffic that it effectively becomes unusable. An attacker will generally demand a payment to stop the DDoS, though numerous security vendors offer protective measures that are relatively effective against them.

The most prevalent type of ransomware will encrypt the files on your system and then demand a ransom (generally in a difficult-to-trace type of online currency like bitcoins) for the decryption key.47 Of course, even if you were to pay the ransom, there’s little incentive for the attackers to actually unlock your data. As with other malware, ransomware attacks start with an ill-advised click on a weblink, attachment, or even an infected USB drive. We will discuss what to look out for when receiving email or browsing the Web in Part II. Thinking before you click (or plug in a stick drive) can go a long way towards preventing an attack like this. In addition to staying vigilant, preparation and prevention are the key considerations in thwarting a ransomware attack. Like the vast majority of malware, ransomware tends to get into a system through older flaws in software that has already been patched by its developers. If your software is kept up-to-date, these attacks are much less likely to succeed. Another critical step is backing up your data (which we will also discuss in Part II). That way, even if you’re hit with ransomware, you can restore your system with your back up files.

Basic protective measures for computer networks include “perimeter” defenses, network monitoring, physical security measures and secure processes. We will cover secure processes in Part II. In the meantime...

Perimeter defenses are focused on stopping attackers before they can get inside your network in the first place or blocking them from accessing protected parts of the network.
Basic firewalls are configured with a set of rules that instruct them whether to accept or reject electronic traffic based upon its source, destination and type of traffic. More advanced firewalls can also look at the traffic in relation to other traffic associated with it, whether it’s coming from essentially an approved sender and, in some cases, the content of the traffic itself. They can be placed just behind the router that effectively acts as the front entrance for electronic traffic coming into your network, on individual computers and servers, as well as at different points in your network to control the type of traffic that can access certain data or resources.

Anti-virus software works by identifying “signatures” (portions of computer code) found in malware. If the anti-virus software encounters a signature it recognizes, it can either block or quarantine the offending program. Attackers are constantly altering malware to try and evade anti-virus software. As a result, anti-virus software – while very helpful – will not completely protect a system by itself. There are a number of effective anti-virus products available, as well as labs that regularly test them for effectiveness.

Whitelisting prevents programs from working on a network unless a network administrator has approved them first (sort of like an invite-only event). It’s effectively the opposite of a blacklist, which blocks programs once they’re identified as bad. Instead, programs will only work once they have been added to the whitelist. While this can be very effective at keeping out malware, the whitelist has to be kept up-to-date. Unless they’re added to the whitelist, legitimate programs won’t be able to run on the system either.

Subnets (short for “subsidiary networks”) are the result of dividing your network into segmented parts, like the watertight compartments on a submarine. Similar to the way a single flooded compartment won’t spread throughout the submarine, an attack infecting a single subnet can be contained before it spreads into other parts of your network. One type of subnet that can pose a significant potential threat if it isn’t properly secured is a guest network for non-employees, like one offering free Wi-Fi access to patients in your waiting room. If you do decide to use one, it must be kept completely separate from the rest of your office network, with no way to access any office files from the guest network.
A DMZ (short for "demilitarized zone") is a type of subnet that effectively sits just behind the entrance to your network. It contains the parts of your network that are directly exposed to the Internet (like your email server), with a firewall between them and the internal network. The idea is that Internet-based attacks can be contained in the DMZ and stopped before spreading throughout the rest of the network.

An air-gap is kind of what it sounds like: keeping a particular computer or other asset physically disconnected from the rest of the network (and not connected via Wi-Fi, either). The theory behind this – even if it gets into the network – an electronic attack can’t bridge the air gap to get to the protected computer or asset. Sometimes this method is used to safeguard computers, external hard drives, etc. holding especially sensitive information.

Unfortunately, no system is completely secure. **Network monitoring** tools analyze systems internally, with the intent of uncovering any intruders as quickly as possible. The monitoring process starts with knowing what’s actually on the network. There are a number of tools that can help your technical staff essentially map out the network and what’s connected to it. It’s also essential to keep an updated list of every computer and device with access to your office network, as well as a list of exactly who can access what. In addition to the dedicated tools designed to monitor and analyze the electronic traffic moving through a network are a number of security tools that can affect that traffic. Here are a few:

- **Intrusion detection systems (IDS) and intrusion prevention systems (IPS)** analyze electronic traffic as it flows through your network. These systems can use digital signatures similar to the ones in anti-virus software or use a behavioral-based approach. The latter entails analyzing the electronic traffic to get a baseline of what “normal” looks like in your network and then reacting when something out of the ordinary occurs. The primary difference between them is a detection system will send you an alert when it encounters something, while a prevention system will try to block it.

- **Data loss prevention (DLP)** software looks for identifying markers found in sensitive data (i.e., credit card numbers, PHI, billing info, etc.) so it can prevent it from moving outside your system. As with other network monitoring tools, DLP software cannot analyze encrypted electronic traffic, but it can be effective in preventing accidental disclosures of sensitive data before it gets outside of your network.

A honeypot is effectively a trap designed to uncover intruders in a network. It can be a dedicated device or software-based and, to someone fishing around a system, it will look like a vulnerable computer or drive with tempting data on it. When an external intruder or malicious insider accesses the honeypot, it alerts the network administrator there’s an intruder poking around the system. That way, steps can be taken to analyze the intrusion and/or boot the intruder from the network.

Logs are electronic records of specific events that occur within an organization’s systems and networks. They can be critical to detecting (or reconstructing) a security incident. System audits would be very difficult to perform without them. Logs can be generated by servers, network security equipment, firewalls and other systems and can generally be set up in a wide variety of ways, including what types of events are logged. Given that they effectively create new log data nonstop, it’s important to balance what data you would like to have with what your system can actually handle.

**Physical security** is a key element in protecting your network. Physical access often equates to network access for even a moderately skilled hacker. And, of course, physical data like handwritten and printed PHI, x-rays, etc. are all vulnerable to an intruder inside the office. Physical security controls fall into three basic categories:

- **Deterrent** – to scare off potential intruders, like a warning sign indicating the presence of an alarm system or security cameras,
- **Detective** – to catch intruders, like a motion sensor or security camera system, and
- **Preventive** – to stop the intrusion, like a gate or locked doors and windows.

One preventive measure you should implement is to physically keep your servers in a separate room or server closet under lock and key and bracketed to the floor. Also, it may sound like something out of a bad movie, but... if your office is in a building
that has drop ceilings, be sure that they can't be used to sneak in after hours.

It's also essential to properly dispose of physical records. Dumpster diving actually does exist. Be sure to shred (use a cross-cut shredder) or otherwise destroy any such records so they cannot be reconstructed before they are disposed of. Remember, if you hire a company to dispose of PHI, you can also be responsible for what happens to it.³⁸

Speaking of disposal, keep in mind that all printers and copy machines have hard drives that can be hacked into. Dispose of them like you would a computer hard drive.

It's also important to effectively check your defenses. This is where vulnerability assessments and “pentesting” come in. Vulnerability assessments center around scans that should be run regularly on the various systems in your network. They essentially check those targeted systems to ascertain what's happening with them, finding weaknesses and “holes” (missing security patches, misconfigured software, etc.) on your systems and networks before the bad guys do. The scans are designed for detection only, though they can be quite helpful at finding out if something unusual is going on. A number of effective vulnerability scanners are available.³¹ The next step, of course, will be fixing the identified vulnerabilities before they can be exploited.

Pentesting is short for “attack and penetration testing.” Pentests are used to test an organization's ability to withstand a simulated attack on its systems. They can be used to test the effectiveness of network monitoring, physical security measures, security awareness training and an organization's response to a security incident. While that sounds pretty cool, pentesting is better suited to organizations with more developed security programs. By nature, pentests are designed to find one way into a network, so the testing won't offer enough information to be a useful early step for a newly forming security program.

Conclusion
The computer, mobile device and network security measures outlined above provide the first steps towards protecting your dental practice. In Part II, we will build on this foundation and discuss the essential importance of secure day-to-day processes in safeguarding your office; tricks hackers use to sneak into computer systems (and offices, too); the right way to use passwords; unexpected dangers lurking on the Web; and how to be prepared for a security emergency.
Course Test Preview
To receive Continuing Education credit for this course, you must complete the online test. Please go to:

1. HIPAA requires patient notification when there has been a data breach, unless ___________.
   a. the office suffering the data breach takes immediate remedial steps in accordance with statutory requirements
   b. the data was encrypted at the time it was stolen
   c. the office suffering the data breach offers theft prevention and credit monitoring services to those affected by the data breach
   d. the data did not include financial information

2. What type of information is the most valuable to cyber criminals?
   a. Credit card data.
   b. Social Security numbers.
   c. Protected Health Information.
   d. They have roughly the same value.

3. A dental practice can assign ultimate responsibility for HIPAA Privacy and Security Rule Compliance to an outside vendor.
   a. True
   b. False

4. What is ciphertext?
   a. Password management software.
   b. A fake website.
   c. A security device that analyzes electronic network traffic.
   d. Encrypted data.

5. Approximately how many pages of text can a gigabyte hold?
   a. 7,500
   b. 500
   c. 75,000
   d. 600,000

6. When you delete a file on a computer _______________.
   a. the indicator showing where the file is on the computer is removed, but the actual file contents remain on the hard drive until overwritten by new data
   b. the contents of the file are destroyed and not recoverable by any method
   c. the file is also deleted from any other place it has been stored
   d. the file is overwritten on the computer's hard drive

7. What is degaussing?
   a. The potentially damaging effect that a mobile device can have upon an airplane's navigation systems if it is turned on mid-flight.
   b. A term used to describe the reorganization of data on a disk drive.
   c. A method of destroying data stored on a magnetic-based storage drive, device and/or tapes by exposing them to a strong magnet.
   d. Scanning the computers in a network for vulnerabilities.
8. **What is the most common sign that a computer has been compromised?**
   a. A pop-up window warning that your computer has been infected.
   b. Nothing.
   c. An audible alarm warning from your computer.
   d. The cursor on the computer starts moving on its own.

9. **What steps should be taken to safeguard the information on a smartphone or other mobile device in case it's stolen?**
   a. Back up the data on the device so that it can be restored in case of theft.
   b. Set a passcode or password and keep the autolock period brief.
   c. Enable remote wiping to destroy the data on the device if necessary.
   d. All of the above.

10. **What is jailbreaking?**
    a. Disabling the preset software and security settings on an iPhone or iPad to allow it to access apps and other content restricted by the manufacturer (Apple).
    b. The physical theft of a laptop or other electronic device.
    c. Breaking into a system electronically to steal data.
    d. Using a smartphone as a mobile Wi-Fi hotspot for a laptop or other electronic device.

11. **A factory reset is designed to electronically remove all data and downloaded applications from a mobile device.**
    a. True
    b. False

12. **Pentesting is ___________.**
    a. an analysis of data used by firm personnel
    b. a simulated attack on a computer network
    c. a test that verifies if a network connection is running properly
    d. a test to see if firm personnel are in compliance with written security policies

13. **Top rated commercial grade antivirus software is all you need to protect a system.**
    a. True
    b. False

14. **A business email compromise relates to an attacker taking over an employee's email account.**
    a. True
    b. False

15. **An endpoint is ___________.**
    a. a quarantine area for malware caught by an antivirus program
    b. data that has been decrypted
    c. the last step of incident response procedure
    d. an individual computer or device connected to a network

16. **An attacker can steal electronic data from a printer or photocopier.**
    a. True
    b. False
17. **What is a honeypot?**
   a. A booby-trapped website.
   b. A type of subnet containing the parts of your network that are directly exposed to the Internet.
   c. A security device (or software) used to detect a network intruder.
   d. A trick email used to tempt the recipient into clicking on a link to an infected website.

18. **A Trojan is __________.**
   a. an encrypted smartphone
   b. a security warning that appears if you are about to click on an infected link
   c. a network security device
   d. a type of malware hidden within something that appears to be safe
References

About the Author

Scott Aurnou, CIPP/US, CIPT

Scott Aurnou is a cyber security consultant, attorney and vice president at SOHO Solutions. He spent over a decade as a litigation attorney in the NYC area, served as lead counsel for a private client services group with Smith Barney, and provided consulting and management planning services for security startup AEI. Scott uses his legal, cyber security, and business background to make information security concepts understandable (and even entertaining on occasion) for non-technical audiences. He has published security related articles in national publications ranging from the New York Law Journal to SC Magazine. Scott has created and delivered numerous presentations on security and privacy issues for executives, managers, and non-technical professionals.

He is a Certified Information Privacy Technologist (CIPT), Certified Information Privacy Professional (CIPP/US) and is admitted to practice law in New York, Colorado, the U.S. District Courts for the Eastern and Southern Districts of New York; as well as the U.S. Court of Appeals for the Second Circuit. Scott is the author of the Introduction to Information Security LiveLessons video training series for Pearson Publishing.