Secure your reputation with secure-mail

Author_ Dr. Lorne Lavine

_Your success hinges on your reputation. Patients remain loyal, or refer your clinic, because of how they feel about the care you provide.

They want to feel they're receiving the most appropriate care, and they want to feel you have their best interests at heart. The way you communicate with patients can significantly influence their feelings in both categories.

By using secure-mail to keep patients and colleagues informed, you can strengthen and protect your reputation because you 1. Are able to more quickly inform patients about their care so they see you as a thorough practitioner (plus, as we know, more informed patients are more satisfied), and 2. Demonstrate your commitment to protecting patient privacy – a concern more and more important to everyone.

_Secure-mail is familiar and new

Although there is more than one service on the market called Secure-Mail, secure-mail is actually a product category. The idea behind these services is that you can share information in a way that is very similar to the user experience of email – data is shared via text or attachment; there's a compose, reply and forward button; you have a contact list; and notifications usually arrive in the inbox of your regular email.

Unlike traditional email, secure-mail services protect the privacy of the information contained within the message, eliminating the threat of a HIPAA breach.

The way secure-mail builds in compliance and protects privacy is by keeping the patient-specific information that you exchange off the public Internet – where it can easily be intercepted and read by unintended and unauthorized recipients.

Messages are stored in a central location that senders and receivers log in to using a web browser (such as Explorer, Firefox or Chrome) so they can securely access the information shared with them.

The similarity to email is no accident. Everyone already knows how to use email, so implementing this technology into your office is effortless. More importantly, text-based email-like exchanges are preferred by patients and colleagues over phone, fax and mail for ease of use, accessibility and tracking of information, and the fact that communication doesn't require alignment of schedules.

For you, it saves time and money associated with calling, faxing and mailing or sending files via courier.

(Photo/Brian Lary, *www.freeimages.com*)

_How to choose your secure-mail vendor

As in any product category, you'll find a range of quality in secure-mail services. This list of important considerations will give you the ability to quickly separate the top from the bottom and decide on an option that will secure your reputation while also providing the desired clinic efficiency.

1. Usability: The service should feel a lot like email. You want to get your new communications up and running with minimal interruption to your productivity. Look for a proven platform that has already made improvements to the user interface based on user feedback. The best user experiences usually come from providers who are specialists in communication software rather than, say, a company that also builds websites.

2. Support: At some point, you will need help with the system. Ask providers what their support availability is, what response times are and how quickly they typically resolve problems. You will also want to choose a service that supports the patients and colleagues you invite to use the service; otherwise, when patients have trouble, it's you they'll call for help.

3. True HIPAA compliance: Remember, encryption does not mean compliant. You are required to have a compliance officer in your clinic. Have them review the requirements and quiz vendors on their approach to protecting patient data and ensuring HIPAA compliance.

4. Integration: To optimize the boost to your productivity, look for a solution that integrates with your practice management software. Integration will save time and data entry workload for your staff. This is not a deal breaker.

Established, well-thought-out secure-mail services easily work with most practice management software but may require a few extra clicks to get information where you need it to go.

5. Attachment size matters: Many files dental practices need to send are high-resolution scans that exceed the limits of regular email anyway. Some secure-mail providers allow large attachment sizes of 500mb or more — plenty of room for any collection of files you'll ever need to send.

Another consideration while we're on the topic of size is storage space. Because HIPAA mandates storage for seven years, you want to steer clear of providers that limit the amount of data they'll store for you or charge extra for additional space.

6. Free use for invitees: In order to get benefits from a secure-mail service, everyone you send messages to must have free access to receive, view and reply. If a provider requires the other end to pay, your subscription will be essentially useless._