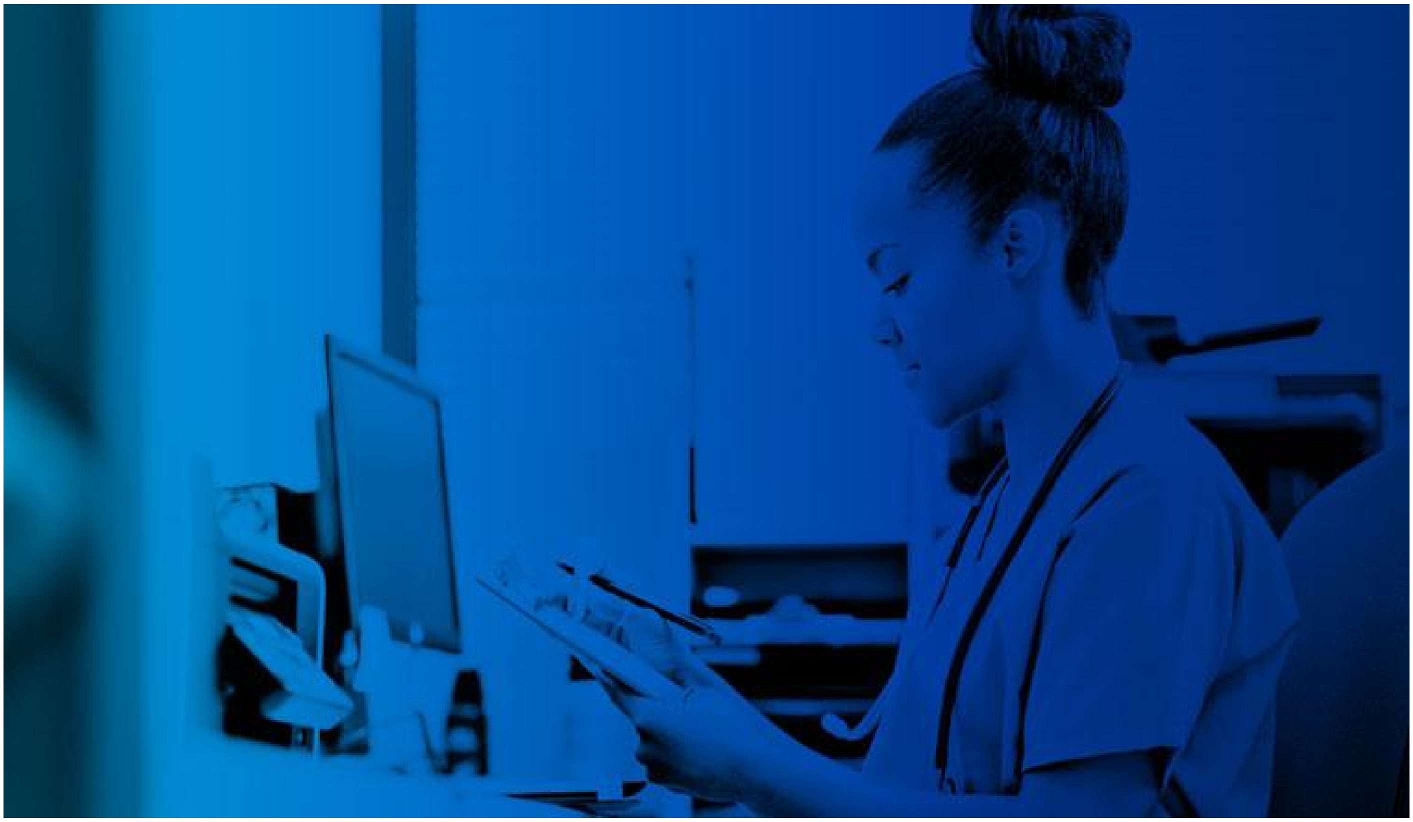
Electronic Communications in Healthcare

August 17, 2016



Managing the flow and security of information in a medical practice

Electronic communication creates liability in mainly two ways: failing to protect confidential information and failing to transmit essential information. The first gets more discussion, but the second causes greater harm. We have seen many claims—and more serious ones—regarding vital messages that did not reach somebody who needed it. When in doubt, err on the side of communicating.

Messaging is either synchronous (real-time, with no storage) or asynchronous (when the content is held somewhere for retrieval). A phone conversation is synchronous. A fax is asynchronous. Emerging standards demand protection for electronic messages both in transit and at rest. It is important to keep in mind that “static” data (documentation, result reporting, etc.) has different risks when it’s in transit.

Dr. Michael Victoroff wrote an excellent white paper called “Electronic Communication in Medical Practice.” It is a great resource and available for download on the MagMutual Patient Safety Institute’s website. Guidelines to Consider Your cyber security plan should describe how you protect all sensitive data that leaves your devices. Some starter questions:

- Do you have secure email for internal communication among your staff and associates?

- What are your practices for email (and other data exchange) with external professionals?
- Do you use a dedicated application for secure text messaging, or do you use the standard app that came on your phone?
- Do you have patients sign an informed consent document before exchanging email with them?

It’s a bigger job to encrypt the static material on PCs, laptops, cellphones, tablets, flash drives, network servers and backups. Because these devices are so regularly penetrated, lost and stolen, there is strong pressure to encrypt every device that contains sensitive data. This means more than just activating the device password, which can often be easily bypassed.

It means making the disk, drive or chip unusable without the encryption key. This is annoying and burdensome, costly in time and training, and causes secondary problems. But, today, it’s hard to defend a breach of an unencrypted device, since the hazard is so well recognized. Your cyber security plan should consider encrypting all devices storing Protected Health Information (PHI). Some starter questions:

- Do you have a policy about which devices are authorized to be used for PHI?
- Do you know where all your PHI is, at all times? In what ways could your PHI-containing devices be compromised? (Threats and vulnerabilities.)

Ironically, it’s possible that the convenience of asynchronous messaging might sometimes be a barrier to communication. As our inboxes swell with notices, results, reports, requests, invitations (and copies of copies), the certainty of missing, deleting or mishandling critical content grows. Simply firing off an email does not guarantee it will be received, appreciated or acted upon.

When patients are injured by dropped tasks, both the sender and the receiver can retrospectively be blamed for not doing more to insure the information got properly acted upon. The “Inbox Problem” is likely to become a serious issue for patient safety. As old fashioned as it is (with the miseries of hold music and “pick-a-number” robots) sometimes think of using that old, synchronous telephone.

Created by MagMutual from materials provided by COPIC as part of MagMutual and COPIC’s alliance to improve patient safety and quality of care for all of our PolicyOwners.

The information provided in this resource does not constitute legal, medical or any other professional advice, nor does it establish a standard of care. This resource has been created as an aid to you in your practice. The ultimate decision on how to use the information provided rests solely with you, the PolicyOwner.

Source URL: https://www.magmutual.com/learning/article/electronic-communications-healthcare