



HIPAA Compliant IT for Independent Providers

Sample Email Confidentiality Notice

WARNING: CONFIDENTIALITY NOTICE - The information enclosed with this transmission are the private, confidential property of the sender, and the material is privileged communication intended solely for the individual indicated. If you are not the intended recipient, you are notified that any review, disclosure, copying, distribution, or the taking of any other action relevant to the contents of this transmission are strictly prohibited. If you have received this transmission in error, please notify us immediately at (xxx) xxx-xxxx or xxx@xxxxxxx.com.

Sample Email Security Warning To Patients

Please keep in mind that communications via email over the internet are not secure. Although it is unlikely, there is a possibility that information you include in an email can be intercepted and read by other parties besides the person to whom it is addressed.

Please do not include personal identifying information such as your birth date, or personal medical information in any emails you send to us. No one can diagnose your condition from email or other written communications, and communication via our website cannot replace the relationship you have with a physician or another healthcare practitioner.

Sample Response To Email From Patient If No Encryption Is Available

Regulations require encrypted messaging systems for confidential communications. Since our e-mail/text communications are not encrypted, it is the policy of [Practice Name] not to use e-mail/text for sharing confidential information. We are sorry if this causes inconvenience for you in receiving information from us.

Please call us at (xxx)xxx-xxxx. Further information about our practice can be found on our website at www.xxxxxxx.com

If you have a medical emergency, please dial 911.



HIPAA Compliant IT for Independent Providers

Further Email Information

“The Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so. See 45 C.F.R. § 164.530(c). For example, certain precautions may need to be taken when using e-mail to avoid unintentional disclosures, such as checking the e-mail address for accuracy before sending, or sending an e-mail alert to the patient for address confirmation prior to sending the message.”

What if a patient initiates communications with a provider using email? The OCR says:

“Patients may initiate communications with a provider using e-mail. If this situation occurs, the health care provider can assume (unless the patient has explicitly stated otherwise) that e-mail communications are acceptable to the individual. If the provider feels the patient may not be aware of the possible risks of using unencrypted e-mail, or has concerns about potential liability, the provider can alert the patient of those risks, and let the patient decide whether to continue e-mail communications.”

Must providers acquiesce to use of email for communications with patients?

Note that an individual has the right under the Privacy Rule to request and have a covered health care provider communicate with him or her by alternative means or at alternative locations, if reasonable. See 45 C.F.R. § 164.522(b). For example, a health care provider should accommodate an individual’s request to receive appointment reminders via e-mail, rather than on a postcard, if e-mail is a reasonable, alternative means for that provider to communicate with the patient. By the same token, however, if the use of unencrypted e-mail is unacceptable to a patient who requests confidential communications, other means of communicating with the patient, such as by more secure electronic methods, or by mail or telephone, should be offered and accommodated.

The OCR also interprets the HIPAA Security Rule to apply to email communications.

“The Security Rule does not expressly prohibit the use of email for sending e-PHI. However, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI.

The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and



HIPAA Compliant IT for Independent Providers

appropriate means to protect e-PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for e-PHI to be sent over an electronic open network as long as it is adequately protected.”

To summarize the rules that apply to HIPAA and email ...

- Email communications are permitted, but you must take precautions;
- It is a good idea to warn patients about the risks of using email that includes patient health information (PHI);
- Providers should be prepared to use email for certain communications, if requested by the patient, but must ensure they are not exposing information the patient does not want shared; and
- Providers must take steps to protect the integrity of information and protect information shared over open networks.