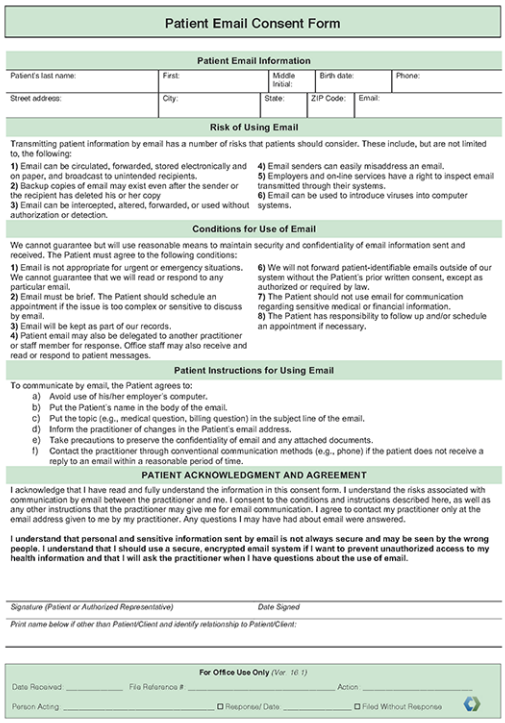
Compliant Solutions

P.O. Box 7933
Tacoma, Washington 98417
www.compliantsolutions.org

Using the Patient Email Consent Form



Patient Email Consent Form

Patient Email Information

Patient's last name:	First:	Middle Initial:	Birth date:	Phone:
Street address:	City:	State:	ZIP Code:	Email:

Risk of Using Email

Transmitting patient information by email has a number of risks that patients should consider. These include, but are not limited to, the following:

1) Email can be circulated, forwarded, stored electronically and on paper, and broadcast to unintended recipients.
2) Backup copies of email may exist even after the sender or the recipient has deleted his or her copy
3) Email can be intercepted, altered, forwarded, or used without authorization or detection.
4) Email senders can easily misaddress an email.
5) Employers and on-line services have a right to inspect email transmitted through their systems.
6) Email can be used to introduce viruses into computer systems.

Conditions for Use of Email

We cannot guarantee but will use reasonable means to maintain security and confidentiality of email information sent and received. The Patient must agree to the following conditions:

1) Email is not appropriate for urgent or emergency situations. We cannot guarantee that we will read or respond to any particular email.
2) Email must be brief. The Patient should schedule an appointment if the issue is too complex or sensitive to discuss by email.
3) Email will be kept as part of our records.
4) Patient email may also be delegated to another practitioner or staff member for response. Office staff may also receive and read or respond to patient messages.
6) We will not forward patient-identifiable emails outside of our system without the Patient's prior written consent, except as authorized or required by law.
7) The Patient should not use email for communication regarding sensitive medical or financial information.
8) The Patient has responsibility to follow up and/or schedule an appointment if necessary.

Patient Instructions for Using Email

To communicate by email, the Patient agrees to:

a) Avoid use of his/her employer's computer.
b) Put the Patient's name in the body of the email.
c) Put the topic (e.g., medical question, billing question) in the subject line of the email.
d) Inform the practitioner of changes in the Patient's email address.
e) Take precautions to preserve the confidentiality of email and any attached documents.
f) Contact the practitioner through conventional communication methods (e.g., phone) if the patient does not receive a reply to an email within a reasonable period of time.

PATIENT ACKNOWLEDGMENT AND AGREEMENT

I acknowledge that I have read and fully understand the information in this consent form. I understand the risks associated with communication by email between the practitioner and me. I consent to the conditions and instructions described here, as well as any other instructions that the practitioner may give me for email communication. I agree to contact my practitioner only at the email address given to me by my practitioner. Any questions I may have had about email were answered.

I understand that personal and sensitive information sent by email is not always secure and may be seen by the wrong people. I understand that I should use a secure, encrypted email system if I want to prevent unauthorized access to my health information and that I will ask the practitioner when I have questions about the use of email.

Signature (Patient or Authorized Representative) *Date Signed*

Print name below if other than Patient/Client and identify relationship to Patient/Client:

For Office Use Only *(Ver. 16.1)*

Date Received: _____ File Reference #: _____ Action: _____

Person Acting: _____ ☐ Response/ Date: _____ ☐ Filed Without Response

Legal Background

The Health Insurance Portability and Accountability Act (HIPAA) regulations governing privacy and security create conflicting messages for health care practitioners concerning the use of email. Generally, practitioners must ensure the security of protected health information particularly when the information will be transmitted electronically. Nevertheless, HIPAA grants the patient a right to request and receive records through an unsecure email account so long as the practitioner warns the patient that it's probably a bad idea.

To be more precise, here is the HHS question and answer regarding the use of email with patients.

"Does the Security Rule allow for sending electronic PHI (e-PHI) in an email or over the Internet? If so, what protections must be applied?"

"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 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***." [emphasis added]

These standards apply to covered entities like health care practitioners and not to patients. Remember that patients may use their own information any way they choose and can authorize any use by others. Consequently, HHS advises that when patients initiate email communication with a practitioner:

> "***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." [emphasis added]

Contrast the HHS advice with the coming audit standard for reviewing a practitioner's security policies and procedures for health information transmission security:

> "Obtain and review policies and procedures regarding the encryption of electronically transmitted ePHI. Evaluate the content relative to the specified criteria to determine that the implementation and use of encryption appropriately secures electronically transmitted ePHI."

> **Standard - [§164.312(e)(2)(ii):** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.]

The federal agency responsible for implementing electronic health record usage offers this additional advice for small practices in responding to the transmission encryption standards:

> "***Based on your required risk analysis***, is encryption needed to protect the transmission of EPHI between your office and outside organizations? If not, what measures do you have in place to ensure the protection of this information? Some small providers might consider password protection of documents or files containing EPHI and/or prohibiting the transmission of EPHI via email." [emphasis added]

In contrast to all these security requirements and warnings to practitioners, HHS underscores the patient "right" to use unsecure email and the practitioner obligation to comply.

> "It is ***expected*** that all covered entities have the capability to transmit PHI by mail or e-mail (except in the limited case where e-mail cannot accommodate the file size of requested images), and transmitting PHI in such a manner does not present unacceptable security risks to the systems of covered entities, ***even though there may be security risks to the PHI while in transit*** (such as where an individual has requested to receive her PHI by, and accepted the risks associated with, unencrypted e-mail). Thus, a covered entity may not require that an individual travel to the covered entity's physical location to pick up a copy of her PHI if the individual requests that the copy be mailed or e-mailed." [emphasis added]

Yet, despite these statements about a patient's right to use unsecure email, HHS reminds covered entities of their liability for breaches arising from use of unsecure email without warning patients:

> "In addition, except in the limited circumstance described below, covered entities must safeguard the information in transit, and are responsible for breach notification and may be liable for impermissible disclosures of PHI that occur in transit. The only exception arises when an individual has requested that the PHI be sent to the third party by unencrypted e-mail or in another unsecure manner, which the individual has a right to request. ***As long as the individual was warned of and accepted the security risks to the PHI associated with the unsecure transmission, the covered entity is not responsible for breach notification or liable for disclosures that occur in transit***."

Practically speaking, what should a practitioner do in light of these conflicting standards?

Summary

Health care practitioners should obtain and maintain a secure email account with a service provider that signs a business associate agreement acknowledging that the email provider follows HIPAA security standards for transmission and storage of protected health information.

In addition, and depending upon the email service features for file sharing, practitioners should separately encrypt sensitive documents before attaching and sending by email (e.g., encrypting a Word document or PDF file). Secure email services often include the ability to upload encrypted documents and have patients securely log into a website to download the information. Practitioners should direct patients to use practitioner secure email and should implement security policies and procedures that require clinic staff from using ONLY the approved secure email account without forwarding.

Finally, practitioners should require patients to read and sign an email consent form whenever the patient insists on using email and whenever the practitioner agrees to use email communication with a patient. The consent form provides required warning to patients about unsecure email and provides the practitioner with evidence of compliance with the warning requirement. Similarly, email signatures should include a reference to the practitioner's secure email and a security warning.