



Quick Links

[CAP Home](#)

[Risk E-Notes Archive](#)

[CAPsules Archive](#)

[CAP Risk Management
& Patient Safety](#)

[Contact Us](#)



Guidelines to Avoid HIPAA and California Regulatory Violations When Sending Protected Health Information via E-mail

It is becoming more and more common for physicians to use their personal e-mail accounts to communicate with patients. Those who do should be aware of, and avoid, potential HIPAA violations and California state regulations designed to protect the security of the e-mail.

E-mails containing Protected Health Information (PHI) should comply with the HIPAA Security Rule, as well as California state regulations regarding transmission of data via e-mail. Failure to do so may constitute violations of privacy and of HIPAA.

Complying with the HIPAA Security Rule means you have policies and procedures in place to protect the security of the e-mail. The Cooperative of American Physicians, Inc. makes the following recommendations:

- **Protect information by encryption** - The HIPAA Security Rule does not specifically mandate encryption. However, the rule requires that the provider implement protections equivalent to encryption, or clearly document why the implementation does not apply. Cost may not be the primary reason for failure to implement the specification.
- **Control access of transmitted information** - Inform the patient as to who in the practice will have access to the e-mail. In addition, the patient should confirm the e-mail address that he or she will be using for doctor-patient communications.
- **Preserve integrity of each e-mail** - Have policies and procedures in place to save and store e-mail to and from patients.
- **Know what type of information you can send** - California law allows some types of reports, lab test results, and other data to be transmitted via e-mail. Make sure you know what information California law does and does not allow to be sent via e-mail.

Because of increasing concern over confidentiality of patient information and of identity theft, encryption is likely to become necessary and required in the future. In the last several years, encryption technology has become much more mature and is no longer cost-prohibitive - even for the smallest medical practices.

Physicians who elect to send PHI via unencrypted e-mail should at least limit the amount and type of information sent through unencrypted e-mail.

For more information about the HIPAA Security Rule, go to Q3 at: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/safeguards.pdf>

Authored by
Ann Whitehead, RN, JD
CAP Risk Management & Patient Safety Department

If you have questions about this article, please use the "Contact Us" button to the left.

Published comments of this information should not be considered legal advice applicable to a specific situation. Legal guidance for individual matters should be obtained from a retained attorney.