Ceretec

HIPAA and the CareConnect

Understanding the Health Insurance Portability and Accountability Act (HIPAA) and how it affects communication with the CareConnect is important to you and your healthcare providers. The underlying structure of the CareConnect is the same as a personal computer, capable of receiving emails from both trusted healthcare providers as well as from friends, family and acquaintances. For completely encrypted email communication between you and "Covered Entities" (those required to follow HIPAA guidelines), equipment at both ends of the email message must have the key to the encryption lock to read the message.

Covered Entities that are required by law to protect your personal health information include:

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
• Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies	• Health insurance companies • HMOs • Company health plans • Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' health care programs	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

This means that emails between you and your family, or you and friends, is not required by law to be protected, even if it includes protected information. In an open email system, as is implemented in most computers, encryption locks are not typically used so that you can read emails from anyone and they can read yours.

However, Ceretec has implemented several features in the CareConnect system to provide protection of your personal health information at all times with specific limitations. Your email address on the CareConnect is created by the Ceretec server. It is a unique and random set of letters and numbers that in themselves have no meaning or identification. The database that links your identification to your email address is entirely separate from the email server that moves your email. All email addresses on the email server belong to a single Ceretec name so that any email that is intercepted, or if the email server is hacked, the identity of any email is not associated with you.

Additionally, the CareConnect server strips off all hyperlinks within emails sent to the CareConnect. This eliminates the potential for viruses or Trojan horse programs to embed themselves in the CareConnect and capture any information exchanged by the CareConnect.

However, these protection steps do not protect you or your provider if you or they "identify you" within the email message. As long as you are not identifiable within the message, test results, prescription information, appointments, etc. contained in the message, cannot be linked to you. It is completely your decision as to whether this communications method is acceptable to you. Additionally, although emails to each individual in your home are stored in separate email boxes, just as with written mail, anyone in the household is capable of opening your email.

For a better understanding how the government interprets the HIPPA regulations, the following paragraphs address questions and answers from the government Health and Human Services website:

7241 Garden Grove Blvd
Suite G
Garden Grove, CA 92841

Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?

Answer:

Yes. 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. 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. Further, while the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail. In addition, covered entities will want to ensure that any transmission of electronic protected health information is in compliance with the HIPAA Security Rule requirements.

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. 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.

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.

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?

Answer:

The Security Rule does not expressly prohibit the use of email for sending e-PHI. However, the standards for access control, and transmission security 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 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.

In addition to what is explained above, you can visit this HHS website that explains your rights as a consumer. http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html

In Summary from the CareConnect End User License Agreement

The HIPAA 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. Certain

7241 Garden Grove Blvd
Suite G
Garden Grove, CA 92841

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. The CareConnect email system has been designed to be HIPAA compliant but with certain limitations. All information connecting your email address to you personally is stored separately from the email server that supports your CareConnect. This server complies with the HIPAA rules and is secured as required by these regulations. If an email message is intercepted, it will not be possible from the email address to identify you. While there is no personal information stored with the assignment of your email address in the CareConnect mail server system, the content that you or your health care providers insert into any email is not encrypted. Additionally, any other members of your household or visitors that have access to your CareConnect will have access to all messages received or sent. ACCORDINGLY, SHOULD YOU OR YOUR HEALTHCARE PROVIDER DECIDE TO USE THE CARECONNECT TO COMMUNICATE MESSAGES CONTAINING PERSONAL HEALTH INFORMATION, YOU, AND NOT CERETEC, ASSUME FULL RESPONSIBILITY FOR THE SECURITY OF THAT INFORMATION. Further you shall indemnify and hold CERETEC harmless from any and all damages, liabilities, costs, and expenses, including reasonable attorneys' fees and amounts paid in settlement of third party or government claims, incurred by CERETEC as a result of or in any way arising from such use.

Note that you have the right under the Privacy Rule to request and have a covered health care provider communicate with you by alternative means, such as by more secure electronic methods, or by mail or telephone. If you initiate communications with a provider using e-mail, the health care provider can assume (unless you have explicitly stated otherwise) that e-mail communications are acceptable to you.

7241 Garden Grove Blvd
Suite G
Garden Grove, CA 92841