Update 8/2016

EMAIL POLICY

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

- 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. 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 at 45 C.F.R. Part 164, Subpart C.

- 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.

- 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.

- http://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/

Clarification in plain English from the US Department of Health and Human Services, HIPAA final rule 2013:

- "We clarify that covered entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email.

- We do not expect covered entities to educate individuals about encryption technology and the [sic] information security. Rather, we merely expect the covered entity to notify the individual that there may be some level of risk that the information in the email could be read by a third party.

- If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request. Further, covered entities are not responsible for safeguarding information once delivered to the individual."

Greenlake Email Policy

- It is the policy of Greenlake Primary Care to attach the following to all company email and (preferably) have patients or patient representative fill out HIPAA email consent:

- "Patients may initiate communications with a provider using e-mail. This email is not encrypted. There may be some level of risk that the information in the email could be read by a third party. If you still prefer unencrypted email, you have the right to receive protected health information in this way, and Greenlake Primary care is NOT responsible for unauthorized access of protected health information while in transmission to you based on this request. Further, Greenlake Primary Care is NOT responsible for safeguarding information once delivered to the you. By replying to this email we will assume (unless you have explicitly stated otherwise) that e-mail communications are acceptable to you.

- HIPAA stands for the Health Insurance Portability and Accountability Act

- HIPAA was passed by the U.S. government in 1996 in order to establish privacy and security protections for health information

- Personal Information is not stored on our computers

- Most popular email services (ex. Hotmail®, Gmail®, Yahoo®) do **not** encrypt email

- When we send you an email, or you send us an email, the information that is sent is **not encrypted**. This means a third party may be able to access the information and read it since it is transmitted over the Internet. In addition, once the email is received by you, someone may be able to access your email account and read it.

- Email is a very popular and convenient way to communicate for many people, so in their latest modification to the HIPAA act, the federal government provided guidance on email and HIPAA. The information is available in a pdf (page 5634) on the U.S. Department of Health and Human Services website: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

The guidelines state that if a patient has been made aware of the risks of unencrypted email, and that same patient provides consent to receive health information via email, then a health entity may send that patient personal medical information via unencrypted email.

OPTION 1 – Allow encrypted email

I understand the risks of unencrypted email and do hereby give permission to Greenlake Primary Care to send me personal health information via unencrypted email.

_____	_____	_____
Signature & Date	Printed name	Please print email address

(parent or guardian if patient is a minor)

OPTION 2 – Do not allow encrypted email

I do not wish to receive personal health information via email.

_____	_____	_____
Signature & Date	Printed name	Please print email address

Please bring completed form to your visit.