

## Guidelines for Email

St. Luke's Hospital (SLH) values and respects the privacy and security of our patients, and we work hard to protect our patients and keep their information safe while it is in our control. You have asked that SLH communicate with you by email. We are providing you with these *Guidelines* so you understand the risks and benefits of email communication, including if you are asking for communication by unencrypted mail.

**Before we begin, remember:** email is not a substitute for personal treatment or other medical care. SLH cannot guarantee that emails will be read and responded to within any particular period of time. It is your responsibility to follow-up with the recipient or schedule an appointment, if needed. **You should never use email for medical emergencies or other time-sensitive matters. Contact your provider in person or by phone, or call 911 in an emergency.**

**There are risks with communicating over the Internet or using email.** There is no guarantee of confidentiality when communicating by email. You are responsible for taking those risks, a few of which are listed below:

- Emails can be intercepted, changed, forged, forwarded, stored, or used without your permission or knowledge.
- Emails can be immediately broadcast worldwide and/or posted on the internet or other public networks.
- Emails can be accidentally misdirected and senders can easily send an e-mail to the wrong address.
- Employers and online services may have a right to store and read emails sent through their systems.
- Email can be used to send viruses, malware, or other harmful codes into computer systems.
- Unencrypted emails are not as secure as encrypted emails. Please be advised that email from SLH will be sent to you **encrypted in a secure email**. If you request otherwise, then you are agreeing that you understand and accept the risks of doing so.

**You are responsible for the privacy and security of your communications, your email accounts, and your devices. You might consider:**

- Taking steps to keep emails private, such as using screen savers and not telling others your computer password.
- Limiting or avoiding use of computer and WiFi's that are not under your control to communicate private information, such as those provided at internet cafes or libraries.
- Protecting your password or other means of access to email, and limiting who can access your accounts.

**When emailing with St. Luke's Hospital, you agree to do the following:**

- Provide us with an accurate email address and notify us in writing if it changes.
- Put your name in the body of the email so we know who is sending it.
- Put information in the email's subject line for routing purposes (such as "billing question" or "medical record").
- Send us a reply message or delivery receipt when we email you so we know you have received it.

**There may be limits on what we provide you in email.** For example, SLH may not be able to honor requests to email sensitive information, such as sexually transmitted diseases, HIV/AIDS, mental health, developmental disability or substance abuse.

**We may also place your email communications in your medical record.** We may also forward them to other providers for your care or to our staff and agents as necessary for treatment, payment or operational purposes.

**In asking us to email you, you understand and agree that SLH** is not responsible for the security and confidentiality of email communications once it leaves our control, including what you do with the information, what happens to the information both in transit and upon arrival, and who else sees the information. You agree to waive and release SLH, our locations, officers, employees, agents, and representatives from all claims, liability, damages costs and fees relating to the emailing of your information, including unauthorized access or other issues related to choices you have made or direction you have given.

**These *Guidelines* may be updated from time to time.**