POLICY AND PROCEDURES CO022 SLHS

POLICY TITLE: **HIPAA Acceptable Use**

POLICY:

St. Luke's workforce members are encouraged to make effective use of information technologies in support of patient care, communications, research, and operations. Authorized access to information is allowed for these purposes. Consistent with other St. Luke's policies, this policy is intended to cover the rights and obligations of the use of data and information.

St. Luke's computing and network resources are to be used only for related patient healthcare, communications, research and operations activities. The computing and network facilities of St. Luke's are limited and should be used wisely and carefully with consideration for the needs of others. Computers and network systems offer powerful tools for patient healthcare, communications, operations and research. When used appropriately, these tools enhance medical care delivery, operations and communications. When used unlawfully or inappropriately, however; these tools can infringe on the rights of others.

St. Luke's cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic resources and communications are warned that they may come across or be recipients of material they find offensive.[1]

This policy is designed to establish acceptable and appropriate use of computer and information systems, networks and other information technology resources at St. Luke's.

SCOPE:

This policy applies to the St. Luke's Health Plan, St. Luke's workforce, and all locations where St. Luke's Health System or its subsidiaries conduct business and/or care for patients. These locations include inpatient and outpatient locations that are part of St. Luke's Boise, St. Luke's Meridian, St. Luke's Magic Valley, St. Luke's Wood River, St. Luke's McCall, St. Luke's Jerome and St. Luke's Elmore.[1] A facility, business or contractor that is affiliated with St. Luke's Health System or one of its subsidiaries may also use this policy if its processes are consistent with this policy and a different policy has not been implemented.

DEFINITIONS:

Workforce Members: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

St. Luke's requires all members of the health system to use electronic communications and information in a responsible manner. The following acceptable use requirements, though not covering every situation, lay out the responsibilities that accompany computer use at St. Luke's and/or on networks to which St. Luke's is connected.

This policy applies to the St. Luke's Health Plan, St. Luke's workforce, and all locations where St. Luke's Health System or its subsidiaries conduct business and/or care for patients. These locations include inpatient and outpatient locations that are part of St. Luke's Boise, St. Luke's Meridian, St. Luke's Magic Valley, St. Luke's Wood River, St. Luke's McCall, St. Luke's Jerome and St. Luke's Elmore.[1] A facility, business or contractor that is affiliated with St. Luke's Health System or one of its subsidiaries may also use this policy if its processes are consistent with this policy and a different policy has not been implemented.

FOR OFFICE USE ONLY			
Originator:	Compliance	Original Date:	12/08/09
Revised Date:	09/27/13, 11/20/13, 12/20/13, 07/31/14		
Effective Date:	09/30/13		Page 1 of 4

I. FUNCTIONALITY AND AVAILABILITY

You shall assure that your actions and the computers you own or that are assigned for your use do not negatively impact the functionality and availability of St. Luke’s computer systems, enterprise and application systems, and network services. Responsible use of computing and network resources requires users to realize that any attempt to misuse these resources could result in degradation of systems or performance elsewhere on the network. You shall not disrupt routine operations by tampering with any hardware, networks, applications, system files or other users' files without authorization or permission; circumventing or altering software or physical protections or other restrictions placed on computers, networks, software, applications or files. Similarly, you may not make resources available to circumvent or alter software protections or other restrictions placed on computers, networks, applications or files. [2]

II. COMPUTER ACCOUNTS

You shall use only your own computer account(s), and may not attempt to impersonate the identities of others. You may not obtain another's password in order to gain access to computers or network systems, data or information. The negligence or naiveté of another person in revealing an account name or password is not considered authorization to use. You may not use the convenience of file or printer sharing as justification for sharing a computer account. You shall not attempt to subvert the restrictions associated with your computer accounts or network access.

III. INFORMATION SECURITY

You are responsible and accountable for all use and security of the electronic resources you manage or use, including but not limited to, computer account(s), passwords, workstations, personal computer(s), laptops*, USB thumb drives/memory sticks*, electronic data*, network access, and any remote access devices such as Blackberries*, smart phones*, PDAs*, etc. You should make appropriate use of the software, system and network-provided protection features and take precautions against others obtaining access to your computer resources. You are responsible for the security of all Network IDs, accounts and passwords assigned for your use. Passwords shall never be shared. You are expected to abide by the St. Luke’s Information Security Policies.

* *Whenever electronic Protected Health Information (PHI) may be exposed to unauthorized access, the appropriate approved and available SLHS encryption technology is to be utilized. Please contact Information Technology for assistance.*

IV. SHARED RESOURCES

You may not encroach on another's use of computer resources. Such activities would include, but are not limited to, tying up computer and network resources; sending harassing messages; sending frivolous or excessive messages, including broadcast messages, either locally or over the Internet; using excessive amounts of storage; launching attacks or probes, or otherwise attempting to subvert the security of any system or network at St. Luke’s or on the Internet; intentionally or irresponsibly introducing any computer viruses, worms, Trojan Horses, spy ware, or other rogue programs to hardware, software, systems or networks at St. Luke’s; or physically damaging systems.

V. INTELLECTUAL PROPERTY

You are responsible for making use of software and electronic materials in accordance with copyright and licensing restrictions and applicable St. Luke’s policies. You may not use St. Luke’s networks, equipment and software to violate copyrights or the terms of any license agreement. No one may inspect, modify, distribute, or copy proprietary data, directories, programs, files, disks or software without proper authorization.

VI. PERSONAL INFORMATION

You should be cautious about making information about yourself and others available on the Internet. St. Luke’s cannot protect you from invasions of privacy, identity theft and other possible dangers that could result from your distribution of personal information.

VII. SOCIAL NETWORK SITES

It is not appropriate to take personal digital pictures or record information regarding patients or personnel and post them on social network sites, such as Twitter, Facebook, MySpace, etc.

VIII. ADMINISTRATION AND IMPLEMENTATION

While respecting confidentiality and privacy, St. Luke’s reserves the right to examine all St. Luke’s owned and operated computer systems and electronic/digital resources. St. Luke’s takes this step to enforce its policies regarding harassment and the safety of individuals; to prevent unauthorized reproduction or distribution of proprietary software or digital texts, and images (moving and still); to safeguard the integrity of computers, networks, and data either at St. Luke’s or elsewhere; and to protect St. Luke’s against seriously damaging consequences.[3] St. Luke’s may restrict the use of its computers and network systems for electronic communications when faced with evidence of violation of St. Luke’s policies, or federal or local laws. St. Luke’s will comply with, and respond to, all validly issued legal process, including subpoenas. St. Luke’s reserves the right to limit access to its networks through St. Luke’s -owned or other computers, and to remove or limit access to material posted or distributed on St. Luke’s -owned computers.

IX. ENFORCEMENT

All members of St. Luke’s are bound by federal and local laws relating to harassment, copyright, security and other statutes relating to electronic media. It should be understood that this policy does not preclude enforcement under the laws and regulations of the United States of America or the State of Idaho. All users are expected to conduct themselves consistent with these responsibilities and all other applicable St. Luke’s policies. Abuse of computing and/or network privileges will subject the user to disciplinary action and sanctions, as established by the applicable operating policies and procedures of St. Luke’s. Abuse of networks or computers at other sites through the use of St. Luke’s resources will be treated as though it occurred at St. Luke’s. When appropriate, restrictive actions will be taken by system or network administrators pending further disciplinary or legal action.

X. OTHER RESOURCES

A. Reporting incidents of electronic abuse to:

1.	The System Privacy Officer at	208-493-0383
2.	The Compliance Hotline	1-800-729-0966
3.	The System Information Security Officer at	208-381-5039

B. Spam may be forwarded to: SpamRelief@slhs.org

C. St. Luke’s Human Resources Employee Handbook, including but not limited to:

"Corrective Action"
"Personal Conduct"
"Confidentiality"

D. Technical Assistance: HelpDesk@slhs.org

XI. FOOTNOTES

[1] *Incidents may be reported to HelpDesk@slhs.org. For more information on this and system and e-mail protections, see "Other Resources" above.*

[2] *Employees who are Systems and Network Administrators in the course of their jobs may be authorized to make changes to computing and network facilities. These responsibilities are well documented, understood and carefully supervised. Users shall coordinate and receive approval from an authorized St. Luke's Information Technology Manager before any changes are made.*

[3] *Upon termination of a user's relationship with St. Luke's, St. Luke's may find it necessary to examine such resources.*

RELATED DOCUMENTS:	Appendix A: Copyright in the Information Age Appendix B: The 10 Most Dangerous Things You Can Do Online Appendix C. The Difference Between Pii and Phi

.AUTHORIZED BY: Original signed by Steven Pitts 09/27/13
System Compliance Officer Date

Interim Change/Annual Review Sheet

Date Changed	Interim Change(s)	Author
11/20/13	Added References and Keywords from Approval Application.	Margaret Stewart Policy Process Analyst
12/20/13	Updated SCOPE, FOOTER, and Policy number to meet system requirements (was IM067 SLHS.)	Margaret Stewart Policy Process Analyst
07/31/14	Added Appendix C: The Difference Between PII and PHI	Herman Doering, HIPAA Security Officer

The following list of supporting references is attached to the foregoing policy for the convenience of staff. This list is not part of the foregoing policy and may not include all resources that were used to research the subject of the policy or prepare the content of the policy. St. Luke's process for developing policies and the content of policies is proprietary business information and may only be shared outside of St. Luke's with permission from a St. Luke's Director, Vice President or CEO, or as required by law.

REFERENCE LIST
HIPAA Security Rule 45 CFR Part 164.308. 310, and 312

KEYWORDS:	functionality, availability, shared, security, intellectual, copyright, personal, spam, computer