Hospital: RSFH System-Wide	**Reference #:** IT. AUP.0001
	Origination Date: 10/1/2012
	Latest Review/Revision: February 2021
	Administrative Approval (Type Name): Laishy Williams-Carlson
	Administrative Title: Vice President/ Chief Information Officer
Division: Information Technology	**Originator (Title):** Chief Information Officer

Subject: **Technology Resources Acceptable Use Policy**

Applicability Statement:

RSFH System: This policy applies to Roper Hospital, Bon Secours St. Francis Xavier Hospital, Roper St. Francis Mount Pleasant Hospital, Roper St. Francis Hospital-Berkeley, and any departments owned or operated by these Hospitals, as well as Roper St. Francis Physician Partners Network, and Roper St. Francis Medshare.

An authorized representative of each group not covered by the *RSFH Administrative Policy and Procedures Manual* (e.g., affiliates, vendors, contractors, etc.) will be required to sign the *Vendor/Contractor/Affiliate Security Policy Disclosure* form verifying that all employees of their company performing work at RSFH must abide by this Acceptable Use policy.

Transmittal of patient information via RSFH technology resources is subject to the RSFH Patient Rights policies for Confidentiality of Protected Health Information (PHI), including but not limited to, applicable administrative policies.

Monitoring is a right, but not a duty, of the RSFH IT team. Monitoring includes without limitation any activity performed on a RSFH technology resource, including but not limited to, Internet sites visited, material downloaded/uploaded by Users to/from the Internet, email sent and received by Users, phone and/or paging records, and voice mail.

Purpose:

Roper St. Francis Healthcare (RSFH) relies on its technology resources to support its business processes and functions. This policy sets forth procedures for the appropriate use of RSFH technology resources by its teammates, independent contractors, agents, and other Users.

Policy:

1) It is each User's duty to use RSFH technology resources responsibly, professionally, ethically, and

lawfully. A User's ability to access RSFH technology resources does not implya right of access. Users should only access RSFH technology resources for which they have authorization via job description function.

2) Each User is responsible for the security of the technology environment. This responsibility extends to the content of communications the User accesses, generates, disseminates or solicits through any RSFH technology resource. This can include, but is not limited to, written reports, faxes, emails, images, photographs, voicemails, and verbal communication.

3) Each User is responsible for ensuring that the use of external computers and networks (e.g., Internet, personally owned devices, home networks) do not compromise the security the RSFH technology resources.

4) Users do not have an expectation of privacy in anything Users create, store, send, or receive on technology resources. Users waive any right of privacy in anything Users create, store, send, or receive on RSFH technology resources, through the Internet or any other RSFH computer network.

5) Prohibited Activities.

    i) Communication of Confidential Information

        (1) Users will not be permitted to store any confidential information including PHI on Internet file shares (e.g., email, file transfer, Google Docs or Drop Box).

        (2) Text messaging communications must not be used to transmit PHI unless the communication is sent via a RSFH approved messaging solution.

    ii) Inappropriate or Unlawful Content

        (1) Content that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, discriminatory, hostile, suggestive, defamatory, or otherwise unlawful or inappropriate may not be downloaded or sent by email or any other form of electronic communication (such as Internet postings, newsgroups, chat groups, voice mail, paging system, music, graphic and video files) or displayed on or stored in any RSFH technology resource.

    iii) Prohibited Uses

        (1) RSFH technology resources may not be used for dissemination, display or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (viruses), political material, or personal data such as songs, videos, photos, accessing suspicious links or any other use prohibited by this Policy.

        (2) Users must not alter the "From:" line or other attributes of origin information in email, messages, or postings with malicious intent. Users must identify themselves honestly and accurately when sending e-mail.

        (3) The sharing of user IDs, ID badges and passwords is prohibited.

        (4) Users must not open or attempt to open the encasement of any technology resource, nor otherwise circumvent any lock system that secures the device or its components.

        (5) Users must not add any type of device inside RSFH facilities (such as a modem, high speed access, wireless access point and/or interface, cellular broadband device) to any technology resource without prior approval from the RSFH Director, Information Security.

        (6) Users must not connect to the RSFH Network by any means other than by those specifically defined by the RSFH Director, Information Security.

        (7) Users must not disable or alter technology resource configurations or functions (e.g., login screens, passwords, virus scan, distribution software, time-out settings, screensavers, wireless networks) unless directed to do so by Information Technology.

        (8) Users must not conduct network mapping, discovery, port scans, traffic analysis, traffic logging or any other information gathering/discovery technique from any RSFH technology resource device unless that action is specifically authorized in their normal duties and responsibilities and approved by the RSFH Director, Information Security.

        (9) Users must not maliciously destroy or otherwise damage, alter or delete any software licensed to or owned by, or any hardware owned, leased, or otherwise in the possession of RSFH. Any

such damage or destruction shall subject User to disciplinary action under this Policy. In addition, RSFH reserves the right to seek compensation through legal action for any damages maliciously caused by User.

(10) Users must not create traffic that would interfere with or adversely affect wireless communication with the RSFH Network (e.g. streaming, bit torrent or another peer to peer communication.

(11) No email communication between any Patient and RSFH teammate will be forwarded to any third party outside RSFH. RSFH teammates will not forward, send, reply to, or otherwise deliver Patient email using any equipment, software or device. For the limited purposes of diagnosis, treatment, payment or healthcare operations, RSFH teammates may forward internally within the RSFH internal secure network email communication received by a Patient or containing information about a Patient. Any spreadsheets or other electronic documents containing confidential information must be password protected and associated passwords must not be contained in any related emails.

iv) Waste of Technology resources

(1) Users must not deliberately perform acts that waste technology resources or unfairly monopolize technology resources to the exclusion of other Users. These wasteful acts include, without limitation, sending non-business related mass distribution emails or chain letters, subscribing to non-business related mailing lists, excessive amount of texting, tweeting, spending excessive amounts of time on the Internet, playing computer games, listening to unauthorized radio broadcasts over the Internet, or otherwise creating unnecessary network traffic.

(a) Exception

(i) Occasional, limited, appropriate personal use of technology resources is permitted when the use does not:

1. Interfere with the User's work performance.
2. Interfere with any other User's work performance.
3. Have an undue impact on the operation of the RSFH technology environment.
4. Violate any other provision of this or any other RSFH Policy.

v) Misuse of Software

(1) Users *must not* do any of the following without prior approval of the RSFH Director, Information Security or Chief Information Officer (CIO):

(a) Copy software for use on home computers

(b) Provide copies of software to any non-RSFH entity

(c) Install software on any technology resource

(d) Download unauthorized software or files from the Internet to any technology resource

(e) Download any software, fames, ringtones, Apps, etc. that result in a cost to RSFH. Reasonable personal use of non-business-related software on RSFH owned cell phone or smart phones is permitted if it does not interfere with the operation of the device or adversely impact the RSFH Network. Software downloads should be limited to commonly available commercial products to minimize the potential for infections from malware or viruses from unknown sources.

(f) Modify, revise, transform, or adapt any licensed software

6) Use of Electronic Devices

a) The use of electronic devices such as camera phones, digital cameras or audio or video recorders to transmit or record confidential images or conversations must be encrypted, password-protected and follow the requirements of the administrative policy, Policy 34, Consent to Treatment, Operation/Procedure, Anesthesia and Use and Disclosure of Protected Health Information For Treatment, Payment, Other Health Care Operations if possible. If not possible, RSFH Director, Information Security or Chief Information Officer (CIO) approval required.

7) Business Access

a) Access will be granted to technology resources per the function as described in the job description.

b) All RSFH systems access privileges will cease when a User's employment or association with RSFH terminates. All system access privileges will be promptly revoked at the time the User's employment or association terminates. In the case of termination by RSFH of the User, all access privileges are denied immediately upon notification. Use of information gained during association or employment with RSFH in any form ceases when the relationship with RSFH terminates.

c) Passwords

i) A unique, separate login account consisting of an ID and password is required for each User of the technology environment, unless otherwise approved by the RSFH Director, Information Security or Chief Information Officer.

ii) Users are required to change passwords upon initial login, upon compromise and as often as required by the RSFH IS department.

iii) Passwords should be at least 12 characters in length and contain at least one numeral or symbol character as outlined within the RSFH Password Policy.

iv) Users are responsible for safeguarding their passwords for access to RSFH technology resources.

v) Individual passwords must not be printed, stored online, on a personal mobile device or given to others.

vi) Users are responsible for all transactions made using his or her User ID.

vii) No User may access RSFH technology resources using another User's account or when another User is logged in.

viii) Users are responsible for locking or logging out of RSFH Network resources when leaving them unattended.

ix) Users must never reveal their passwords to anyone for any reason and never enter their RSFH network credentials into an external website.

8) Security

a) Physical Security.

i) Users must always take all reasonable and prudent measures to physically secure all technology resources.

ii) Users must use the provided lock down kit to secure laptops and tablet computers whenever the device is stationary.

iii) Mobile devices and removable media must always remain with the owner or be locked a secure place when not in use.

iv) Mobile devices and removable media must be stored in a locked vehicle's trunk, where available, while being transported and must not be left in the trunk overnight or for long durations. Never leave items lying in a vehicle that are visible from the outside.

v) Users must report any lost or stolen technology resources, such as removable media, laptops, cell phones, smartphones and other mobile devices, including personally owned devices used to connect to the RSFH Network to the IT Helpdesk immediately.

b) Encryption of Mobile Devices and Removable Media

i) All RSFH issued mobile devices that access the RSFH Network, including email, will be provisioned with RSFH Director, Information Security approved encryption software.

ii) Mobile devices must employ device-level user authentication that engages after no more than 15 minutes of inactivity.

c) Copiers, Printers, Scanners, Fax Machines, etc.

i) Office equipment that contains flash memory, a hard drive or both for processing and storing electronic data, must have appropriate safeguards in place to minimize exposure of confidential information and PHI when the equipment is used, stored, moved, disposed of, lost or stolen.

ii) Any security feature inherent to the equipment, such as encryption and/or data overwrite/wipe, must be enabled.

iii) Rented or leased equipment must be sanitized of all data in accordance with IT Equipment Disposal Procedure before being returned to the vendor.

d) Equipment Disposal

i) Before any device with internal storage (e.g., servers, PCs, mobile devices, digital cameras, medical monitoring equipment, routers, network monitoring devices, removable media, Storage Area Network devices (SAN), fax machines, copiers, and printers) are transferred outside the immediate department, returned to surplus inventory or a vendor, or discarded, the storage media must be cleansed of all data in accordance with IT Equipment Disposal Procedure.

e) Cameras

i) The use of patient photography, videotaping, digital imaging, and other visual recordings of patients taken by the clinician during patient care for clinical purposes is allowed in accordance with Corporate Policy 86, Authorization to Review and Release Protected Health Information Policy.

ii) Any images that identify the patient (e.g., full face photographic image, placard with patient name and medical record number) are considered PHI and must always be properly secured.

iii) When at all possible, remove any patient identifiable features or information from the scene before recording the image.

iv) Cameras and other recording devices that contain patient images as well as removable storage media must be stored in a secure location to prevent theft.

v) All data contained on these devices should be removed promptly after completion of use and never stored for long periods of time.

vi) Storage media that contains patient images – memory cards, film, USB storage devices, etc. – must be disposed of in accordance with IT Equipment Disposal Procedure.

vii) Loss or theft of a camera or other recording device, or media containing patient images must be reported to the IT Helpdesk immediately.

f) Downloading Patient Identifiable Information.

i) Users must take all reasonable and prudent measures and are responsible to ensure the safety and confidentially of all patient identifiable information downloaded to any communications device, (e.g. smartphones, digital camera, computers, laptops, and removable media). Reasonable measures include but are not limited to storing files and databases only on a RSFH Network share wherever possible.

(1) Instances where sensitive data cannot be stored on a network share and must be stored locally on a computer or mobile device will require the use of whole disk encryption or other Information System approved encryption method.

(2) Password protecting sensitive files, using an approved encryption method

(3) Employing any additional measures as directed by the IT department.

ii) Any non-RSFH person that downloads patient identifiable information, for example a consulting physician, is considered a covered entity and is solely responsible for protecting the safety and confidentially of the data.

9) Bring Your Own Devices

User's access to and continued use of personal mobile devices to access the RSFH Network and network resources is granted on the condition that each User follows these requirements:

i) Personal mobile devices may require the installation of software to enable access to RSFH Network resources. This software allows Information Technology to remotely erase RSFH data on the device. It is recommended and incumbent upon the user to backup personal data in an encrypted format to ensure personal data is safeguarded and restorable. RSFH will not be liable for personal data that may be lost as a result of remotely erasing RSFH data.

ii) RSFH reserves the right to remove RSFH data on personal devices at any time, and RSFH data will be erased upon termination of employment or association with RSFH terminates.

iii) User will not download or transfer PHI or other confidential information to their personal devices. This excluded RSFH email that is protected using encryption.

iv) User will password protect the device requiring authentication after no more than 5 minutes of inactivity.

v) User will configure the device to perform a complete erase of all data on the device after 10 failed login attempts.

vi) User will maintain the original device operating system and keep current with security patches and updates, as released by the manufacturer.

vii) User will not "Jail Break" or "Root" the device or otherwise install software that allows the User to bypass standard built-in security features and controls.

viii) User will not share the device with family members or other unauthorized individuals, due to the business nature of the device and potential access to RSFH data.

ix) User will delete any PHI or other confidential information that may be inadvertently downloaded and stored on the device through the process of viewing email attachments.

x) User will comply with the litigation hold requirements outlined in Information Management and Retention Policy.

xi) User must notify the RSFH IT Helpdesk, within one hour or as soon as possible, when a mobile device is lost or stolen. User will not disable service with the carrier until the RSFH IT Helpdesk has confirmed the device has been successfully wiped.

10) Policy Governing Specific Applications

i) Following is a list of specific applications and how each should be used acceptably by RSFH teammates. This is by no means an exhaustive list of applications. The general spirit set forth below will be applied consistently across any new technologies, or new uses of technologies. If the situation or technology you are concerned about is not listed below, please contact either the RSFH Director, Information Security or the RSFH Chief Information Officer for specific direction regarding the acceptable use of your application.

a) Email Usage

(i) Any email being sent outside of RSFH, over the Internet, that contains business confidential or PHI must use a RSFH approved encryption method. (i.e., using the "Send Secure" button versus "Send").

(ii) Emails containing social security numbers must be encrypted using RSFH

approved encryption methods.

(iii) Phishing emails often attempt to use triggers to get the recipient to react quickly without thinking through whether they should respond or not. This may include dire language as time has run out, alleged requests from RSFH Leadership, loss of service or penalties for not responding, or a request for money. The phishing emails may have grammatical, spelling, and syntax errors, as well as phrasing a native speaker would not use.

An example of a phishing email may include a generic greeting warning of a change in an account requiring verification of account information. These emails typically include directions to reply with private information or may provide a link to a web site to verify the account by providing personal information such as name, address, bank account numbers, Social Security numbers, passwords or other sensitive personal information. As a reminder the RSFH Help Desk will not ask for your username or password.

Indicators of a phishing email:

(i) Sender's name and email address does not match
(ii) Usage of words such as 'Official' to attempt to prove legitimacy
(iii) Usage of a real organization or company name but incorrect an email address
(iv) Poor grammar
(v) Unsolicited requests for personal information
(vi) Misspellings

(iv) Reporting Suspicious Emails

(i) One Click of the Report Suspicious Email button in your inbox.

(ii) On devices which do not provide the above option, such as cell phones, users must simply forward the suspicious email to SuspiciousEmail@rsfh.com. Reporting an email this way is also an alternative option for all other platforms RSFH teammates use to access their email.

(v)What should I do if I have been scammed by phishing?

(i) Contact the RSFH Help Desk at 843-724-2920
(ii) Change your RSFH login credentials
(iii) Attend a mandatory Information Security Awareness training

b) Email Equipment and Software Standards

i) Users are prohibited from using personal email accounts or web-based email (e.g., Yahoo Mail, Google Gmail, Comcast) to transmit or receive RSFH confidential information or PHI.

ii) Mobile Devices

i. Users communicating with Patients via mobile device-based software may only utilize RSFH approved software with all required security measures.

iii) Instant Messaging/Real-Time Communication.

i. Text messaging communications must not be used to transmit PHI unless the communication is sent via a RSFH approved messaging solution.

c) Other Required Email Footers

i) Attorney-Client Communication.

i. Email sent from or to in-house counsel or an attorney representing RSFH should include this warning: "ATTORNEY-CLIENT PRIVILEGED. DO NOT FORWARD WITHOUT PERMISSION."

ii) External Disclaimer.

i. Email sent from the RSFH Network to any outside address will have an approved system generated disclaimer banner attached at the end of the correspondence.

11) Policy Violation

i) Reporting a Violation

a) A User must notify the RSFH Director, Information Security if he or she feels that security may have been compromised in any way. Notification must be made to the RSFH Helpdesk 843-724-2920. When:

(1) Encounters with inappropriate material on the Internet.

(2) Receipt of unwanted or inappropriate communication or solicitations from an outside source.

(3) Users who become aware of any misuse of software or violation of copyright law should immediately report the incident.

b) Possible misuse of patient identifiable information must be reported to the RSFH Corporate Privacy Officer

ii) Violation Investigation

a) The RSFH Director, Information Security and/or RSFH Chief Information Officer are/is responsible for conducting investigations into any alleged technology compromises, incidents, or problems.

iii) Disciplinary Action

a) Any violation of this Policy may lead to disciplinary action. The Progressive disciplinary process shall be in accordance with RSFH's Teammate Accountability & Just Culture policy. Disciplinary action may include without limitation, verbal or written reprimand, termination of employment and/or appropriate legal action.

(1) The RSFH Director, Information Security or RSFH Chief Information Officer may deny or revoke technology privileges if there is reasonable evidence that a violation has occurred.

(2) Security privileges may be restored only after consultation between the RSFH Director, Information Security, RSFH Chief Information Officer and RSFH Management and/or RSFH Senior Management personnel.

(3) Teammates who access and/or obtain patient specific information on any patient other than the patients they are treating, billing for or performing hospital business operations for, will be in violation of the HIPAA Privacy law.

12) Technology Acceptable Use Policy Exceptions

i) Exceptions to this Policy may be made with written approval from both the Director, Information Security and RSFH Chief Information Officer (CIO) and where applicable the Chief Privacy Officer.

Appendix

Confidential – Patient Health Information (PHI), Personally Identifiable Information (PII), Business Information, Payment Card Industry (PCI) or other sensitive information.