INFORMATION PRIVACY, SECURITY, AND TECHNOLOGY RESOURCES

Regional West Health Services and its related entities (collectively, "RWHS") allows authorized persons to have timely and appropriate access to computerized information while safeguarding the information's confidentiality, security, and integrity. Security processes will reduce or eliminate threats to the computer systems and electronic information. All employees and students are responsible for using technology resources properly and maintaining information privacy and security.

Responsibility: Students
Standard: Information Management

I. PURPOSE

Regional West Health Services (RWHS) has adopted this Information Privacy and Security and Technology Resources Policy (the "Policy") to ensure uniform and appropriate use of Technology Resources and Technology Information, both defined below. The rules, obligations, and standards described in this policy apply to all RWHS and related entity employees, medical staff users, temporary workers, independent contractors, students, agents, and other computer or telecommunication users (collectively, the "users", as defined below), wherever they may be located.

It is every user's duty to use RWHS Technology Resources responsibly and in a professional, ethical, and lawful manner, including use in accordance with all applicable state and federal laws and regulations. In addition, every user is responsible for ensuring the privacy and security of RWHS Information Systems and its valuable proprietary and confidential information. Users agree to assist RWHS in investigating any potential or actual violations of this policy.

Violations of this policy may result in disciplinary action, including termination of enrollment in the Program, and potential civil and criminal liability. Use of the Information Systems is a privilege that may be limited or revoked at any time, with or without cause and without notice, in the sole discretion of RWHS. If a user does not accept the terms of this policy, including particularly the provisions regarding collection and use of personal information, the user may be denied use of the Information Systems, may be denied enrollment, or may be terminated from enrollment.

II. DEFINITIONS – See Appendix A

III. **POLICY**

When using or accessing RWHS Information Systems, users must comply with the following provisions:

1. Use of Technology Resources (In General)

Technology Resources and Technology Information constitute a valuable business asset of RWHS and may only be used for approved purposes. Users are permitted access to the Technology Resources to assist them in the performance of their jobs or for education.

2. Confidential / Proprietary Information / Protected Health Information (PHI)

Each user must take all appropriate precautions to insure Confidential/Proprietary Information is not improperly disclosed or otherwise compromised. In particular, each user must use PHI in strict accordance with RWHS established procedures and in conformation with all applicable state and federal laws including, but not limited to, HIPAA and all relevant consumer protection and privacy laws. In the event a person becomes aware of any actual or potential compromise of privacy and security or misuse of PHI, the person must immediately report the incident and any information he or she may have to the Privacy and/or Information Security Officer or the Chief Information Officer, or the person may choose to make a report anonymously through the RWHS Privacy and Security Hotline by phone at **630-1025**. Any consideration of whether or not to report should be resolved in favor of reporting.

3. **Due to the unsecure environment of the Internet, e-mail will not be used for sending confidential patient information to any external e-mail address without data encryption**. Confidential information includes all protected health information, including but not limited to, name, address, account number, social security number, age, etc. To ensure e-mail is encrypted simply type <secure> or <encrypt> in the subject line (important to included carrots).

4. Ownership of Technology Information and Technology Resources

All of the Technology Information and Technology Resources are the sole and exclusive property of RWHS. Any user files, e-mail, and other Technology Information stored on the Technology Resources are the property of RWHS.

5. Limited Personal Use of Technology Resources

Occasional, limited, appropriate personal use of Technology Resources is permitted when the use does not:

a) Interfere with the user's clinical or didactic performance;
b) Interfere with any other user's work or academic performance;

c) Unduly impact the operation of RWHS Information Systems or in any way compromise the security of the Technology Resources;
d) Result in any material expense to RWHS;
e) Violate any law or regulation of any jurisdiction; or
f) Violate any other provision of the policy or any other policy, guideline, or standard of RWHS.

Wireless Internet access of the "guest" wireless network is permitted using personal devices. Generally, the "guest" wireless network should not be accessed during normal clinical or didactic educational periods unless said access is applicable for academic or business reasons.

Users are strongly discouraged from using Technology Resources to store, send or receive information that is personal to them (e.g. online account passwords and activities, communications of a personal nature, visiting Web sites that may identify personal information about the user, etc.). As discussed below, all information transmitted through or stored on RWHS Information Systems may be reviewed by others. RWHS cannot guarantee and does not assume any obligation to protect the privacy and security of this kind of user personal information. If a user desires privacy and security for this type of personal information, the user should not use RWHS Technology Resources. Instead, the user should generally restrict the information to a computer owned and operated by the user (e.g., the user's own home computer).

6. No Expectation of Privacy

Users understand and agree that:

A. RWHS retains the right, with or without cause or notice to the user, to access and monitor Technology Information, including user e-mail, internet usage, and screen level access to all RWHS clinical and business systems. Anything created or stored on RWHS Information Systems may, and likely will, be reviewed. Without limiting the foregoing, RWHS may record and access any use of RWHS Information Systems to measure and set standards for performance of the user's duties; to monitor the user's compliance with applicable laws and this policy; to determine whether specific communications are business or personal communications; and for any other purpose related to RWHS business operations;

B. Password protected, encrypted, and deleted files, including those identified as "private", "personal", or equivalent may be recovered and reviewed;

C. Users have no expectation or right of privacy of any kind related to their use of the Technology Resources or any Technology Information; and

D. Users expressly consent to the access, monitoring, and recording of their use of the Information Systems and any Technology Information, and waive any right of privacy or similar right to their use of RWHS Technology Resources or any Technology Information.

7. Prohibited Activities

7.1 Inappropriate or Unlawful Material

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate, including any comments that would offend someone on the basis of race, age, sex, sexual orientation, religion, political beliefs, national origin, veteran status, or disability, must not be sent by e-mail or other form of electronic communication, including Online Forums, viewed on or downloaded from the Internet or other online service, or displayed on or stored in RWHS Information Systems. Users encountering or receiving such material must immediately report the incident to their supervisor or other responsible manager.

7.2 Prohibited Activities

Users may not use RWHS Information Systems for personal financial gain or the benefit of any third party (including the sale of any non-RWHS business or sponsored activities, or in violation of RWHS policies and applicable laws relating to political activity or lobbying. Technology Resources may also not be used to create, store or distribute any form of malicious software (e.g., viruses, worms, or other destructive code). Users may not install or use encryption software other than that which has been installed or specifically approved by Information Services.

7.3 Music and Video Files; File Sharing Networks

Unless specifically approved for business purposes or otherwise provided with the Technology Resources, the Technology Resources may not be used to download music or video files or any kind (e.g., MP3, WAV, AAC, AFF, WMA, etc.). Users may not access music or video file sharing networks (e.g., Kazaa, Napster, Morpheus, etc.) from the Technology Resources.

7.4 Protection of RWHS Software and Data

Except with approval from authorized RWHS management, users may not upload or transmit any software or data licensed to RWHS to the Internet or any other third party systems.

7.5 Waste of Technology Resources

Users may not deliberately perform acts that waste Technology Resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending non-business related mass e-mailings or chain e-mail, subscribing to a non-business related Listserv, excessive use of Information Systems for non-business related activities (e.g., personal purposes, playing games, engaging in non-business related online "chat groups"), or otherwise creating unnecessary network traffic.

7.6 Large File Transfers

Audio, video, and picture files require significant storage space and may not be downloaded to or stored on the Information Systems unreasonably or unless they are business related. All files that are downloaded must be pre-scanned for viruses and other destructive programs.

7.7 Misuse of Software

Without approval from authorized RWHS management, and excluding automatic updates, patches, and tools installed or approved by Information Services, users may not do any of the following:

a) Copy RWHS owned or licenses software for use on their home computers;
b) Provide copies of RWHS owned or licensed software to any independent contractors or consultants of RWHS or to any third person;
c) Install software or any non-approved updates to any existing software on any of RWHS workstations or servers;
d) Modify, revise, transform, recast, or adapt any software; or
e) Reverse engineer, disassemble, or decompile any software.

Users who become aware of any misuse of software or violation of copyright law must immediately report the incident to their immediate supervisor or other RWHS manager or the RWHS Helpdesk at 630-1188.

7.8 Online Agreements

Without prior approval by authorized RWHS management, users may not accept or agree to be bound by any terms and conditions

of use (other than standard terms and conditions of use for access to Web sites), license agreements, or other types of online agreements, which are in excess of the user's authority for written agreements.

8. Use of Copyrighted Information

8.1 In General

It is the policy of RWHS to prohibit copying or distribution of copies of any Copyrighted Publication of third parties, except as:

a) Permitted by the legal principle of "fair use" (as describe in Section 7.3, below) or

b) Authorized by a contract or license that RWHS has obtained. Copies of all contracts and licenses for Copyrighted Publication should be retained by the appropriate RWHS manager at the location of use and by RWHS legal counsel.

Copying is defined as the use of a photocopy machine, through retyping, faxing, and reprinting, as a result of storage, duplication or printing of electronic information, and through the posting of material on the Internet and other networks.

Distribution is defined as copies of Copyrighted Publications being sent through interoffice delivery, e-mail, Internet transmission, etc. For example, copying of an article from the New York Times Web site and then distributing copies of the article either electronically or in hardcopy to others, including fellow employees, could potentially infringe several of the New York Times' exclusive rights as the owner of the copyright in the article.

8.2 Limitations of Copyright

Copyright does not necessarily protect all forms of information or printed materials, particularly raw data, facts, "ideas", and "processes", and works in the public domain (e.g., works that are very old or that are specifically dedicated to the public domain), so copyright law ordinarily should not preclude users from extracting the base factual information they need to conduct normal business activities. Questions about what is permitted should be directed to RWHS legal counsel.

8.3 Fair Use

"Fair use" is a legal principle that permits a limited amount of copying of Copyrighted Publications to occur, depending on the

facts and circumstances. Based on the ordinary needs of RWHS, "fair use" will more likely occur if the following factors are present:

a) The purpose of the copying is for educational or research use;

b) The copying is a necessary step for extracting, understanding or using data or information (e.g. a necessary step in using a computer program is to copy the program into the memory of the computer);

c) The copying is to create a substantially different work that conceptualizes, analyzes, expands upon or otherwise transforms the material being copied. This is a key element of fair use. It is one thing to simply copy an existing article and distribute it to twenty other people. It is quite another thing to take the ideas in an existing article and to expand upon them in a new article. In the first instance, there will likely be no fair use. In the later instance, the potential for fair use is high;

d) The amount of material being copied is limited to small portions, excerpts, or abstracts (e.g., if a particular paragraph in an article is of interest, do not copy the entire article)

e) The copying is not "systematic" in the sense that copies of the same or similar works are not being made repetitively, continuously, and/or in multiple quantities under circumstances that could be seen to substitute for purchases or subscriptions. The classic example of 'systematic" copying is the monthly copying of the entire contents of a trade journal for circulation to every member of a particular department. That kind of activity would almost certainly not be a fair use;

f) The copying is ad hoc and as needed, conducted within Regional West Medical Center on a per-item basis, and not be commercial copy centers for large-scale distribution; and

g) Distribution of copies is strictly limited, and no fee or charge is collected for the copying or distribution.

The foregoing guidelines state some, but not all, applicable considerations, and do not preclude fair use from existing in other situations. Because every situation is judged separately, each user has final responsibility for exercising sound judgment and reasonable restraint.

Each department of Regional West Health Services, depending on need, should consider establishing more particularized guidelines for limiting the amount of copying that occurs. Any such guidelines must be approved by Regional West Health Services legal counsel before being implemented.

8.4 Copyright Management Information

Users may not alter Copyrighted Publications in such a way as to change, obscure, or remove information relating to the copyright owner, copyright notice information, the author of the work, the terms and conditions of use of the work, or identifying numbers or symbols referring to the foregoing information or links to such information. To the maximum extent possible, users should use electronic links (such as hyperlinks) to reference copyrighted material instead of making copies of such material.

9. Use of Electronic Messaging

9.1 In General

All user e-mail addresses assigned by Regional West Health Services shall remain the sole and exclusive property of Regional West Health Services. Users should endeavor to make each of their electronic communications truthful, accurate, and consistent with the qualities of good business communications. Always allow time to reflect before composing and sending a message. The following guidelines should be followed in drafting e-mail:

a) Avoid using all capitals;

b) Avoid excessive use of bold-faced type;

c) Only mark high-priority items as “priority”;

d) Avoid copying unnecessary parties with the “Reply All” feature;

e) Make the subject line for your e-mail descriptive;

f) Avoid using graphic backgrounds for your e-mail and ornate type fonts. These will make your e-mail less readable and will require far greater company resources to store and transmit than ordinary e-mail; and

g) Do not send messages to all users or other large groups within the company unless business-related and a compelling business reason exists.

9.2 Altering Attribution Information

Users may not alter the "From" line or other attribution of origin information in e-mail or other online postings. Anonymous or electronic communications sent using fictitious names are forbidden. However, a user may specifically grant another user the right to send e-mail on behalf of the grantor (e.g., a manager authorizing her assistant to send an e-mail on her behalf).

9.3 Forwarding Electronic Messages

Users should use their good judgment in forwarding e-mail to any other person or entity. When in doubt, request the sender's permission before forwarding the message. Electronic Messages containing confidential/proprietary information or attorney-client communications may never be forwarded without the permission of the sender or other authorized personnel. All messages written by others should be forwarded "as-is" and with no changes, except to the extent that the changes are clearly indicated in the original text (e.g. by using brackets [ ] or other characters to indicate changes to the text).

9.4 Confidential/Proprietary Information

If confidential/proprietary information is transmitted via the Technology Resources, the sender of the message is responsible for:

a) Ensuring the message is clearly labeled in the subject line the body of the message as "confidential", "proprietary", "confidential: unauthorized use or disclosure is strictly prohibited" or "privileged attorney-client communications";

b) Keeping the number of recipients to a minimum;

c) Ensuring all recipients are aware of the obligation to maintain the confidentiality of the information contained in the message; and

d) Assuring that the transmission of information is in accordance with this policy and applicable law.

9.5 Receipt of Unsolicited, Unintentional, or Misdirected Confidential/Proprietary Information

In the event a user receives e-mail, whether designated as confidential or not, by mistake, the user should stop reading the message and immediately notify the sender or system administrator. It is a violation of this policy to read e-mail intended for another person without the express prior consent of that person or other authorized Regional West Health Services personnel.

9.6 Listserv Subscriptions

Users should be selective in subscribing to listserves and other e-mail distribution lists. It is inappropriate to discuss or reveal confidential information, patient information, customer data, or trade secrets while participating in a Listserv. Some discussion groups are very active and may result in dozens of e-mail every day. Promptly unsubscribe to any listserves that are not actively being read. When subscribing to a listserv, make sure to keep a record of the steps necessary to cancel the subscription. This information is usually contained in an initial message from the listserv, but may not be easily located later.

9.7 Access to Electronic Messages Through Third-Party Devices

Users must be authorized by an appropriate Regional West Health manager to use a pager, PDA, home computer, or third-party device to access their Regional West Health e-mail.

9.8 Restricted Use of Third-Party E-mail Accounts and Services

The use of non-Regional West Health Services e-mail accounts (Personal Webmail, Hotmail, Yahoo, AOL, etc.) must be infrequent, irregular, and temporary. Users may not use alternate, non-Regional West Health Center provided or non-Regional West Health Services authorized e-mail addresses to send business-related message containing confidential/proprietary information or Protected Health Information (PHI).

9.9 Retention and Destruction of Electronic Messages

Each user is responsible for ensuring that his or her use of e-mail is consistent with this policy and Program Policy #722.8.0.15 , Electronic Mail and Telecommunications Usage.

9.10 Violations of Records Management Policy

Electronic messages will be retained in accordance with Program Policy #722.8.01.30 and may be automatically deleted by authorized personnel after 180 days without advance warning. Users may not circumvent storage prohibitions outlined in that policy by sending, forwarding, or copying any e-mail or related documents to themselves or others for the purpose of evading this requirement.

10. **Internet Access and Use**

(Also contained in Program Policy #722.8.01.25, Internet Use)

10.3 Users are encouraged to use the Internet and intranets to assist them in the performance of their jobs or education. The utilization and sending of work related documents to and from personal e-mail systems such as Yahoo Mail, Google Mail, and MSN Mail is strictly prohibited. Accessing social networking Internet sites, such as My Space, Twitter, and Facebook are also prohibited. Authorized uses include, but are not limited to, the following:

a) Client and customer services, human resources staff, education related purposes, and/or for work related research;
b) Electronic communication; and
c) Professional purposes and procurement of information from external sources.

10.3 Internet Monitoring

Regional West Health Services has software and systems in place that are capable of monitoring and recording all Internet usage. For each user, these security measures are capable of recording each Web site visited, each online forum, or e-mail message, and each file transfer into and out of Regional West Medical Services networks, and Regional West Health Services reserves the right to conduct such monitoring and recording at any time. As described in Section 2, users have no expectation of privacy as to their Internet usage. Regional West Health Services will review Internet activity and analyze usage patterns, and may choose to publicize this data to assure that the Information Systems are used in accordance with the provisions of this policy. Regional West Health Services may use software and other technological means to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

10.3 Internet Forums, Online Forums, Listserve and Meeting Sites

Public discussion forums, e-mail subscription lists and collaborative meetings are sometimes referred to as web forums, message boards, discussion, chat rooms, blogs, IM, Listserve subscriptions, Net Meetings, or electronic bulletin boards.

It is inappropriate to discuss or reveal confidential information, patient information, customer data, or trade secrets while participating in one of these forums. Only those users who have been duly authorized by Regional West Health Services may speak/write in the name of the company when making postings to one of these forums. Users must identify themselves honestly, accurately, and completely when participating in one of these forums and when setting up accounts on outside computer systems. Users may participate in forums, provided (i) participation will assist them in the performance of their jobs, (ii) they do not disclose any confidential/proprietary information, and (iii) unless authorized by their supervisor, the user makes no attempt to speak or write on behalf of Regional West Health Services and includes the following footer on all postings or comments:

> *"This posting reflects the individual views and opinions of the author and does not necessarily represent the views and opinions of Regional West Medical Center."*

Each posting leaves an "audit trail" indicating at least the identity of Regional West Health Services Internet servers, and, most likely, a direct trail to the user. Inappropriate postings damage Regional West Health Services reputation and could result in corporate or individual liabilities and may result in discipline.

10.3 Accessing the Internet

To ensure security and avoid the spread of viruses, users accessing the Internet through a computer attached to Regional West Health Services network must do so through an approved Internet Gateway. Accessing the Internet directly, by modem, from a workstation is strictly prohibited unless the computer is not connected to the network (e.g., a laptop being used remotely). Even if a stand-alone computer with a modem is used to access the Internet or other network, the modem must never be left in auto-answer mode.

10.3 Disclaimer of Liability for Internet Use

Regional West Health Services is not responsible for material viewed or downloaded by users from the internet. The internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material.

In general, it is difficult to avoid at least some contact with this material while using the internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the internet may lead to the receipt of unsolicited e-mail containing offensive content. Users accessing the internet do so at their own risk.

11. **Users Working at Home**

Users may be authorized to work at home as a normal assignment or on a limited, as-needed basis. Users authorized to work at home must do so via a Secure Remote Access (SRA) account provided by the Regional West Health Services Information Systems Department. Users are responsible for ensuring that only Regional West Health Services authorized personnel will have access to (i) Regional West Health Services provided computers, (ii) Confidential/proprietary information, including PHI, or (iii) Regional West Health Services system access procedures. All use of home computers to access Regional West Health Services Information Systems must be in compliance with this policy. Users may not copy confidential/proprietary information or PHI to any form of removable media. In the event confidential/proprietary information is reduced to printed form, all copies of such printouts must be returned to Regional West Health Services. Papers containing confidential/proprietary information that are no longer needed may not be disposed of at home. All such papers must be returned to Regional West Health Services for proper destruction.

12. **Passwords**

12.3 Responsibility for Passwords

Users are responsible for safeguarding their passwords for access to the Information Systems. Users should recognize that the combination of a logon identification (user name or user ID) and password is a unique identifier. Individual passwords should not be printed, stored on-line, or given to others. Users are responsible for all transactions made using their passwords. No User may access the computer system using another user's password or account. Students must follow these guidelines for passwords:

a. Do not reveal a password to ANYONE-EVER
b. Do not reveal a password in an e-mail message
c. Do not talk about a password in front of others
d. Do not hint at the format of a password, like "my favorite thing"
e. Do not reveal a password on questionnaires or security forms
f. Do not share a password with family members
g. Do not reveal a password to co-worker or other students

Students must not use the "Remember Password" feature of applications (Outlook, Internet e-mail accounts, Instant Messenger, etc.)

Students are encouraged to avoid writing down and storing passwords anywhere. Further, avoid storing passwords on ANY computer system (including smart phones or similar devices) without encryption.

12.3 Password Guidelines

a. Users should select strong passwords. Strong password have the flowing characteristics:
    1. Be at least eight characters in length
    2. Be a mixture of upper and lower case letter, numbers, and special characters
    3. Be changed at least every 90 days
    4. Be different from previous passwords
    5. Not contain the user's name or user ID

b. Note that poor, weak passwords have the flowing characteristics:

1. The password contains less than eight characters
2. The password is a word found in a dictionary (English or foreign)
3. The password is a common usage word such as:
    a. Names of family members, pets, friends, co-workers, co-students, fantasy characters, and so on
    b. Computer terms and names and commands, websites, companies, hardware, software
    c. Birthdays and other personal information such as addresses and phone numbers
    d. Words or number patterns like aaabbb, qwerty, zyxwvuts, 123321, and so on
4. Any of the above spelled backwards
5. Any of the above preceded or followed by a digit (for example , secret1, 1secret1)

c. Users will be prompted to change their network password every 365 days or whenever a compromise of the password is suspected or any period defined by Regional West Health Services policy

d. Password should not be associated with personal information (e.g., PIN used for bank card, dates of birth for self or family members, telephone numbers, first or last names of self or family member, password used for Internet accounts

12.3 Passwords Do Not Imply Privacy

Use of passwords to gain access to the Technology Resources or to encode particular files or messages does not imply that users have an expectation of privacy in the material they create or receive on the Technology Resources. Regional West Health Services has access to all material stored on its computer system – regardless of whether that material may have been encoded with a particular user's password.

13. **Security**

13.1 **Prohibited Use of Removable Media**

Generally, users should not copy, store, or transfers any "Protected Health Information" (PHI) or "Confidential/Proprietary Information" from any Regional West Health Services technology resources to any form of removable media (e.g. USB drive, Flash Drive, CD, memory sticks, etc.) Under certain circumstances there may be a legitimate business need to copy, store or transfer confidential or protected electronic information. One of the following security

safeguards must be applied prior to copying any PHI or confidential information from a Regional West Health Services technology resource to any form of removable media. Contact the Regional West Information Services **Help Desk at 630-1188** for help on specific solutions and devices.

a) Microsoft Office files (WORD, EXCEL, etc.) Encrypt the file using the Tools/Option/Security/Encryption Password feature. Select "Microsoft Strong Cryptographic Provider" as the encryption method.

b) Encrypt the file and/or storage device using only Regional West Health Services approved removable media or devices. Regional West Health Policy #500.4.118, The Use, Receipt, and Removal of Portable Media and Computing Devices that Contain Electronic Protected Health Information (PHI) and/or other Protected Data" refers.

c) Students who retrieve any PHI in preparation for case studies or other assignments of a course must remove the patient name and other patient identifier before the information is loaded onto any form of removable media (e.g. USB drive, Flash Drive, CD, memory sticks, etc.)

d) Students who retrieve any PHI in a paper format in preparation for case studies or other assignments of a course must remove the patient name and other patient identifier before use or leaving campus

13.2 Accessing Another User's Files

Users may not alter or copy a file belonging to another user without first obtaining permission from the owner of that file. The ability to read, alter, or copy a file belonging to another user does imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of others by unnecessarily accessing personal files and e-mail for disciplinary/performance reviews, authorized security activity and other measures employed by Regional West Health Services to police and protect the Technology Resources and its business.

13.3 Accessing Other Computers and Networks

A user's ability to connect to other computer systems using the Technology Resources or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.

13.4 Control of Removable Media

Users must adhere to established procedures to label, account for, and control all removable media containing Regional West Health Services data or information, regardless of whether such data or information is current or obsolete. Removable media must be stored securely and should never be left unattended. Removable media must be disposed of in accordance with procedures provided within the policy governing their use. Regional West Health Policy #500.4.118, "The Use, Receipt and Removal of Portable Media and Computing Devices that Contain Electronic Protected Health Information (PHI) and/or Other Protected Data" refers.

13.5 Use of Remote Access Software

The installation, set-up and use of software that provides a remote user control of an in-house desktop computer (e.g., Carbon Copy, Close-up, PC Anywhere, Procomm Plus) are **NOT** authorized. Users requiring remote access will conform to item #10 above and contact the Regional West Health Information Services **Help Desk at 630-1188** for assistance.

13.6 Computer Security

Each user is responsible for ensuring that his/her use of outside computers and networks, like the Internet, will not compromise the security of Regional West Health Services Technology Resources. This duty includes taking reasonable precautions to prevent intruders from accessing Regional West Health Services network without authorization and to prevent the introduction and spread of viruses. Users granted access to Portable Technology Resources are responsible for insuring that unauthorized persons are prevented from using such devices for any purpose, including accessing other Technology Resources or the Regional West Health Services network. If any Portable Technology Resources are lost or stolen or if a user believes that a password has been compromised, report the incident immediately to the Regional West Health Information Services Help Desk at 630-1188. Regional West Health Policy #500.4.118, "The Use, Receipt and Removal of Portable Media and Computing Devices that Contain Electronic Protected Health Information (PHI) and/or Other Protected Data"

14 Viruses

Viruses can cause substantial damage to computer systems. Each user is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into Regional West a Services Technology Resources and for timely reporting discovered viruses to the Information Service Help Desk at 630-1188. To that end, all material received on any type of removable media or optical media and all material downloaded from the Internet or from computers or networks that do not belong to Regional West

Health Services MUST be scanned for viruses and other destructive programs before being placed onto Regional West Health Services Technology Resources. Users should understand that their home computers and/or laptops might contain viruses. All media transferred from these computers to Regional West Health Services technology resources MUST be scanned for viruses.

15 Disclosures Regarding Security Issues

In order to prevent subsequent incidents, information relating to virus attacks, hacking incidents and other breaches of security shall be treated as Regional West confidential/proprietary information. Unless specifically directed to do so by authorized Regional West Health Services management. Users may not discuss this information with their co- workers, other students, or disclose it to any non-employee. Reporting Incidents In general, reports about violations of this policy should be directed without hesitation or delay, to the Director of Information Services or the Chief Information Officer. Regional West Health Services users may also choose to make a report anonymously through the Regional West Health Services Privacy and Information Security Hotline by phone at 630- 1025. Any consideration of whether or not to report should be resolved in favor of reporting.

16. Miscellaneous

16.1 Compliance with Applicable Laws and Licenses

In their use of Regional West Health Services Technology Resources, users must comply with all software licenses, copyrights, and all other state, federal, and international laws.

16.2 Other Policies Applicable

In the use of Regional West Health Services Technology Resources, user must observe and comply with all other policies and guidelines of Regional West Health Services, including, but not limited to the following:

- RWMC Policy #500.4.118, The Use, Receipt and Removal of Portable Media and Computing Devices that Contain Electronic Protected Health Information (PHI) and/or other Protected Data.
- RWMC Policy #500.4.104, Privacy Complaint Process.
- Program Policy #722.8.01.25, Internet Use.
- Program Policy #722.8.01.03, Electronic Mail and Telecommunications Use.
- Program Policy #722.8.24.45, Corrective Action

16.3 No Additional Rights

This policy is not intended to, and does not grant, users any contractual rights.17. Violations of this Policy

Failure to comply with this Information Privacy, Security and Technology Resources Policy may result in Corrective Action up to and including termination of access privileges to computer systems and/or termination of enrollment at the discretion of Regional West Health Services management. (Also see Policy 722.8.24.45, Corrective Action). Privacy and/or security investigations are complaint based and will be conducted by the RWHS Privacy Officer and/or the RWHS Security Officer or their designee(s). Whenever possible, the Director of Human Resources, or designee(s), will participate in the investigation and serve as a witness/recorder. The outcome of privacy and/or security investigations will generally be categorized in one of the following levels:

LEVEL 0

The first occurrence of a substantiated privacy and/or security investigation, reveals a student either: (1) ACCIDENTALLY (see definition in Appendix A), or (2) by failing to comprehend and correctly apply teaching, committed, either a privacy or security violation.

LEVEL I

The first occurrence of a substantiated privacy and/or security investigation reveals an student who has either a legal right of access or legitimate business need to access information, knowingly failed to either: (1) use appropriate safeguards or (2) follow proper procedures, resulting in unauthorized access(es) and/or inappropriate disclosure(s) to another RWHS employee. Also includes the second occurrence of a level 0 violation.

LEVEL II

A first occurrence of a substantiated privacy and/or security investigation reveals a student who either had: (1) a legitimate business, work-related need to access and disclose protected health information but failed to use appropriate safeguards or to follow proper procedures that resulted in an inappropriate disclosure outside of RWHS/RWPC/Hospice, or (2) without a legitimate business or work related need to access to protected health information for PERSONAL INTEREST (see definition in Appendix A). Level II violations also include the third occurrence of a level 0 violation or the second occurrence of a level 1 violation.

LEVEL III

A first occurrence of a substantiated privacy and/or security investigation reveals a student who either had not legitimate business or work-related need to access information knowingly and intentionally gained access to protected health information with a goal of PERSONAL GAIN (see

definition in Appendix A) MALICIOUS INTENT (see definition in Appendix A). or 2) without legitimate business, work or academic related need accesses network, application or Internet resources resulting in an actual or potential information security vulnerability. This level of policy violation can include civil and/or criminal penalties. A level III violation also includes the third occurrence of a level I violation or the second occurrence of a level II violation.

Corrective Action

Once the investigation has been completed and the Privacy and/or Information Security officer has determined the level of violation, that information will be reported to the direct supervisor of the student for Level 0 breaches and the Director of HR or designee(s) for level I, II, or III violations. The Director of HR or designee will work with the appropriate manager or Director to prepare and communicate the appropriate corrective action as defined in Program policy 722.8.24.45.

Generally speaking, Level 0 violations would result with a corrective action of early intervention. Level I violations would result in a written warning. Level II violations would result in a final written warning. Level III violations would result in termination of enrollment. However, the facts and circumstances of each situation will ultimately determine the level of corrective action communicated to the student, in accordance with Program Policy 722.8.24.45.

Daniel Gilbert, MSEd, RT(R)(CV)(MR)(CT)(QM), FASRT

Daniel Gilbert, MSEd, RT(R)(CV)(MR)(CT)(QM), FASRT
Program Director

Sharon A. McKinney, M.P.A.

Sharon McKinney, MPA
Director, Imaging Services

Reference Policy: 103.0.06 Medical Center Policy Information Security and Technology Resources

Reviewed: 11/17/2011, 4/26/12, 2/21/13, 1/31/14
Revised: 1/16/15, 1/15/16

APPENDIX A

Responsible Use of Technology and Information Resource Policy
Definitions

As used in this policy, certain terms are defined as follows:

Accidental
Happening by chance and not planned; not specifically intended and arising as a side effect.

Auditability
The ability to do a methodical examination and verification of all information activities such as entering and accessing.

Authentication
The validation of correctness for both the information itself and the individual who is the author or user of information.

Confidential/Proprietary Information
Confidential/proprietary information includes, but is not limited to, any information owned, licensed, or possessed by Regional West Health Services that (i) Regional West Health Services is contractually obligated to protect (e.g., third-party information that is the subject of a confidentiality or non-disclosure agreement); (ii) Regional West Health Services is obligated to protect according to State and Federal law or regulation (e.g., PHI, as defined below); or (iii) is not generally known to the public, especially if such information gives Regional West Health Services a competitive advantage or its disclosure would harm Regional West Health Services. Confidential/proprietary information includes, but is not limited to, trade secrets, proprietary information and all other information, documents, or materials, owned, licensed, developed, or possessed by Regional West Health Services or any employee or agent of Regional West Health Services, whether tangible or intangible, relating in any way to Regional West Health Services patients, prospective patients, business plans and activities, business relationships, costs or profit information or data from which that information could be derived, human resources (including internal evaluations of the performance, capability, and potential of any Regional West Health Services employee), business methods, databases, and computer programs whether or not marked as “confidential” or “proprietary”.

Copyrighted Publications
Copyrighted publication means materials that are subject to protect under the law of copyright. These materials include, but are not limited to, third-party software, software manuals, trade articles, textbooks, newspaper and magazine articles, electronic databases, graphics, audio files, pictures, and material available on the Internet. While having a copyright notice and/or a “©” may provide the copyright owner with additional

rights, they are not required for copyright protection to apply. Almost every document, whether written or electronic, is subject to copyright protection – whether or not it has a copyright notice. When in doubt, users should always assume that a document is copyrighted.

Electronic Messaging
Electronic messaging means messages sent and received via electronic means, either through an internal network or over an external network (e.g., e-mail, instant messaging, Web-mail, Internet Relay Chat ("IRC"), etc.), including any file attachments.

Encryption
Encryption is the process of transforming plain text (readable) into cipher text that is unreadable without a special software key.

Internal Service Provider
Internal Service Provider means a Regional West Health Services department or unit that is providing some kind of information technology service (mail, records, file service, computational cycles, statistical analysis, data access, etc.) to other users within that unit and/or to others outside of that unit.

Internet Gateway
Internet Gateway means a hardware and/or software system placed between the Technology Resources and the Internet to limit unauthorized access to and use of the Technology Resources.

Listserv
Listserv means an automatic distribution method for e-mail on the Internet. Typically a topic-centered discussion list where recipients receive copies of e-mail sent by other subscribers.

Internet or Online Forums
Internet or online forums means online discussion groups, news groups, bulletin boards, chat rooms, blogs (a form of online diary which individuals may post descriptions of their activities), IM, Net Meetings and other similar forums on the Internet and other public networks (e.g., AOL, Google, Yahoo, and MSN).

Malicious Intent
Results when a workforce member has a plan that is motivated by or resulting from a desire (want for something very strongly) to cause harm (physical, mental, financial, moral impairment or social embarrassment) or pain (physical or emotional) to a patient by accessing and/or disclosing protected health information.

Non-Repudiation
Non-repudiation is the inability to dispute a documents content or authorship.

Personal Gain
Profit; to obtain personal advantage from something

Personal Interest
Results when curiousness about the affairs of others results in intentional unauthorized accessing of and/or inappropriate use or disclosure of protected health information.

Protected Health Information or PHI
PHI means information identifiable to a patient, including all information governed by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security and Privacy Standards (45 CFR Part 160, 162 and 164).

Policy
Policy means the Information Security and Technology Resources policy, including all attachments.

Portable Technology Resources
Portable Technology Resources means those Technology Resources that are portable or mobile in nature. By way of example only, Portable Technology Resources include laptops, personal digital assistants (PDAs), palmtop computers, portable/handheld telecommunications devices (e.g., cellular telephones pagers, and radios), cameras (both digital and analog), and other similar devices.

Removable Media
Removable media means portable or removable hard disks, floppy disks, USB memory and hard drives, zip disks, optical disks, CDs, DVDs, digital film memory cards (e.g. Secure Digital (SD), Memory Sticks (MS), CompactFlash (CF), SmartMedia (SM), MultiMediaCard (MMC), and xD-Picture Card (xD)), magnetic tape, and all other removable data storage media.

Server
Server means a computer running administrative software that controls access to a network and its resources, such as printers and disk drives, and provides resources to computers functioning as workstations connected to the network and code that provides a service on the network.

Technology Information
Technology Information means all information, data, and communications created, received, or stored on or passed through the Technology Resources, including all user files and e-mail.

Technology Resources
Technology Resources means Regional West Health Services entire computer and telecommunications network, including, but not limited to, the following: fax machines, host computers, file servers, application servers, communication servers, mail servers, laboratory systems, scanners, fax servers, Web servers, workstations, stand-alone computers, laptops, Personal Digital Assistants (PDSs), palmtop computers, portable/handheld telecommunications devices (e.g., cellular telephones, pagers, and radios), cameras (both digital and analog), software, applications, data files, removable media, and all internal and external computer and communications networks (e.g., intranets, extranets, Internet, commercial online services, value-added networks, e-mail systems) accessed directly or indirectly from Regional West Health Services computer network.

Users
Users means all employees, medical staff, independent contractors, consultants, contract employees, temporary workers, and other persons or entities using the Technology Resources, wherever located or however deployed.

Virus
Virus means a program that infects computer files and systems, often with destructive results (e.g., loss of data, unreliable operation of infected software and systems).

Workstation
Workstation means an individual or shared computer assigned to one (1) or more users.