

Our Community Health Center

Information Management (IM) Policies and Procedures

Our Community Health Center
123 Old Road
City, State Zip

Signature:

Date: _____

I have read, understand, and agree to follow all policies and
procedures within this manual.

Approved by the Board of Directors: April 24, 2007
Implementation: May 8, 2007

The purpose of this manual is to detail all the policies and procedures regarding the Information Management Department.

This manual is divided into distinct sections and organized by a decimal system. For example, Section 100 is “Our Community Health Center Information Management Policies and Procedures: Introduction and Manual Organization”; next is section 101, “Our Community Health Center Information Management Department”. Section 200 begins with “HIPAA and PHI”, an entirely different subject.

Policy 100.1: The Information Management Policies and Procedures will be reviewed on an annual basis.

Policy 100.2: Initially each MIS user will receive a paper copy of these Policies and Procedures.

- You may request additional paper copies of the Policies and Procedures document through IM Department by calling the computer room at ***-***-**** .

Policy 100.3: A copy of this Policies and Procedures manual will be available on the Intranet.

- The IM Policies and Procedures can be found online by going to <http://your website>

Policy 100.4: The Information Technology (IT) staff can bypass or make an exception to any Management Information System (MIS) policy to resolve problems in an emergency situation or if they diagnose the system as being down.

The organization, Our Community Health Center has two Information Management (IM) departments overseen by the Manager of Information Architecture. The first department, Information Technologies (IT) provides application support, data integrity, maintenance, integration design, general training, security, and connectivity. The second department, Management Information Systems (MIS), provides reporting, support and training with specialized data bases.

Per HIPAA legislation, Our Community Health Center is required to have an active Security Officer. Our Community Health Center's Security Officer is the Manager of Information Architecture.

Our Community Health Center's Information System is *nicknamed* "OurHealthNet". The term OurHealthNet, in its broadest use, is defined as any equipment, network operating systems, site to site circuits (T1 Lines), applications, data, Protected Health Information, and any other equipment or data that makes up Our Community Health Center's Information Systems. Its definition also includes any functionality or integration of itself.

OurHealthNet's purpose is to collect, organize, store, maintain, secure, and present data in schemes to reflect the methodology and diverseness of the organizational values. In doing this effectively, OurHealthNet will streamline and enhance the capture and flow of OCHC's data, information, and knowledge and deliver it to individuals and groups engaged in accomplishing work. Further, it will embrace a diversity of knowledge sources, including databases, web-sites, OurHealthNet users, and partners through relating that knowledge where it resides, while at the same time capturing its content and giving it greater meaning through its relation to other information in the organization.

OurHealthNet as of 2007 is a multiple platform computer system that is built off of

DESCRIPTION OF INFORMATION SYSTEMS SHOULD BE HERE

200	The Health Insurance Portability and Accountability Act and Protected Health Information
-----	------------------------------------------------------------------------------------------

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed into law on August 21, 1996 (P.L.104-196). It contains a broad spectrum of legislation that focuses on the following three areas:

- Insurance Portability
- Fraud Enforcement
- Administrative Simplification

Insurance Portability and Fraud Enforcement are non-applicable to Information Management Policies and Procedures. Thus, they will not be covered in this manual. The policies and procedures in this section deal only with the security component of HIPAA.

The Administrative Simplification component of the HIPAA legislation implements regulations for standardizing electronic transactions of health care data. It also contains provisions for the Privacy and Security of personal health information. Administrative Simplification applies to all maintained and transmitted forms of personal health information – including paper, electronic, or oral communications.

Protected Health Information is defined as any individually identifiable health information that is transmitted or maintained in any form or medium by an entity covered under HIPAA. Basically, this means that any information that would go in the patient’s medical record or chart that could be used to identify the patient from a list of other patients with similar information should be considered PHI.

Examples Patient **Protected Health Information** (PHI) includes the following:

- | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Name • Street Address • City • Country • Precinct • Zip Codes • Names of Relatives and employers • Date of Birth • Date of Service • Telephone number • Web URL and IP Address • Biometrics (finger prints, voice prints, iris scan, etc.) | <ul style="list-style-type: none"> • Fax number • E-mail address • Social Security Number • Medical Record Number • Health Plan Beneficiary Number • Account and Chart Numbers • Certificate / License Numbers • Vehicle Identification • Device Identifiers • Photographs • And any other unique identifying number, characteristic, or code (whether generally available to the public realm or not) |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

There are seven basic provisions governing use of PHI:

1. PHI may be used by OCHC for purposes of treatment, billing, or operations related to treatment and billing with or without patient consent.
2. OCHC is required to notify all patients of how PHI is used and to ask all patients for consent to use PHI for any reason (even treatment and billing), but if consent is not granted by the patient, PHI can be used for treatment and billing operations without patient consent.
3. OCHC is required to obtain patient consent for using PHI for any other reason including marketing, fund raising, solicitation for research studies.
4. OCHC is required to obtain authorization from the patient prior to release or disclosure of PHI to the patient’s designee or other entities.

5. If information is disclosed by OCHC, OCHC will make an effort to disclose only the minimum amount of information necessary to meet the needs of the individual or entity requesting the information.
6. OCHC is required to De-identify information what will be used for other purposes if consent has not been granted by the patient.
7. OCHC is required to obtain agreements with any Business Associates who receive PHI that bind the Business Associate to comply with OCHC's information practices policies.

Policy 200.1: Our Community Health Center will establish methodologies for monitoring activities related to the privacy and security of protected health information. OCHC will audit activities related to the privacy and security of protected health information at regular intervals throughout the year.

- Our Community Health Center will monitor the following:
 - Use, disclosure and release of protected health information
 - Access to system and medical records
 - System maintenance activities
 - Document storage and disposal activities
 - Records of each time information is accessed
 - Records of system maintenance activities
 - Records of document storage
 - Hardware and software inventories

Policy 200.2: From time to time, patients will ask that OCHC receive transfers of their PHI electronically from other providers or payers. Our Community Health Center will make every effort to ensure that the electronic transfer occurs in a secure fashion and that records are maintained securely.

- Routine and non-routine transfers of patient information will be treated with the same standards as current electronic medical records are treated.
- The practice will develop a methodology along with its vendor for the receipt, transmission and dissemination of electronic health information.

Policy 200.3: All data transactions that occur through third parties (e.g.: claims clearinghouses or billing agencies) will be subject to the signature of a chain of trust agreement with those parties before data can be transacted or disclosed.

- OCHC's attorneys will develop a "chain of trust" contract for the practice and its third party contractors. This is a contract in which the parties agree to electronically transmit data and protect the transmitted data in ways compliant with HIPAA security standards.
- All third party contractors to whom protected health information is transmitted electronically will be required to sign chain of trust agreements. This agreement does not include referring physicians or hospitals that use data for the treatment or billing for treatment of the patient.
- Contracts will be kept on file in central files. Contracts will be reviewed every three years along with other administrative safeguards.
- Once a year, in order to monitor compliance with the agreement, the security officer of OCHC will contact all chain of trust partners of the practice and ask them to confirm that data being transmitted is secure and that their data practices are HIPAA compliant. Confirmation could include obtaining copies of certification of security practices of the chain of trust partner but it will be left to the discretion of the OCHC security officer to determine sufficient compliance with the chain of trust agreement.

Policy 200.4: OCHC will take reasonable steps to limit the use of disclosure of Protected Health Information.

- This policy does not apply to disclosure requests from referring physicians or health care providers who are treating the patient, the individual who is the subject of the information, standard HIPAA transactions, Department of Health and Human Services (DHHS), and law enforcement officials and other uses or disclosures required by law.
- Access to protected health information and the type of information available will be limited to the OurHealthNet users who need the information to conduct their work duties. The security plan contains a list of OurHealthNet user job descriptions and levels of access to information.
- For routine or recurring requests from payers (for example: requests for chart notes or prepayment reviews) the information released will be restricted to the service in question.
- For non-routine requests, the releasing party will use the following criteria to determine the amount of information that needs to be released:
 - Is the information required to support a claim or receive payment?
 - If information is not released, will it delay quick, effective treatment?
 - Is releasing the information consistent with professional standards protecting the unnecessary sharing of patient information?
- In certain circumstances, the judgment of the party requesting the information may be relied upon to determine the minimum amount of information necessary for its purpose. If the request for information is made by a public official or agency, another provider or representative from a payer or a medical researcher with appropriate documentation from an Institutional Review Board, then the exact information they request can be released to them.
- Any information released in this manner will be subject to verification of the identity of the person requesting the information. Identity can be verified by asking for written requests on company letterhead or request in person with appropriate corporate identification.

Policy 200.5: If protected health information is to be used for any purpose other than treatment, billing or operations related to treatment and billing, the information will be “de-identified” by removing all information that could distinguish the individual’s record from a group of records.

- The patient’s name, address, diagnosis, chart notes, lab results, treatment plan, insurance or financial information are all considered protected health information. All of these elements appearing together could be used to identify a patient.
- It is the responsibility of a OCHC manager to determine the information on a report that could reasonably be used to identify an individual.
- Any information that could uniquely identify the patient will be removed from data printouts or reports. For example: a report to analyze treatment patterns by market could contain zip codes and diagnoses but not patient address or names.
- Patient address information can be used for newsletters and for contacting the patient prior to an appointment but will not be used for targeted marketing activities. For example: the practice could send out quarterly newsletters to its entire patient base but the practice could not develop and send marketing materials to patients who have had a specific treatment plan for a hip injury unless the patients indicate that they would like to receive such targeted materials on their consent forms.

Policy 200.6: Any OurHealthNet user who attempts to bypass such practices as outlined in policies 200.1 through 200.5 will be subject to disciplinary action up to and including possible termination of employment. In the case of a non-employed OurHealthNet user, access to OurHealthNet will be locked-out.

To insure a proper understanding of computer and security policies and procedures OCHC is requiring all OurHealthNet users to attend various computer use, application use, and security training sessions.

Computer Use Training – This will cover general training on general PC and Thin-Client use, Windows use, and other Network Operating System services. This will also cover training on acceptable PC and Thin-Client use.

Application Use Training – This will cover training on the applications that will be made available for the OurHealthNet user by the OCHC Information Technology Department. The OurHealthNet user will also be trained on the proper method / methods of communicating new requests and system problems to the Information Technology Department.

Security Training – This will cover training on Computer, Email, and Internet Security. The OurHealthNet user will also be trained on acceptable PC and Thin-Client use as it pertains to security.

Policy 300.1: Unless an exception is made by the Security Officer in conjunction with the Director of Human Resources, OurHealthNet users must fall within one of the following OurHealthNet user categories to be given access to OurHealthNet. (1) Any authorized employee type as defined in the OCHC Human Resources Manual. (2) Board members.

Policy 300.2: OCHC is requiring all OurHealthNet users and consultants to sign an agreement of confidentiality to prevent unauthorized disclosure of sensitive business and technical information including but not limited to work in progress, work planned concepts, know-how and trade secrets specifically relating to health care and health care information systems. The term OurHealthNet user in this policy *excludes* OCHC Board of Trustees.

300.2.a: Employees. As a condition of employment, Our Community Health Center will require all employees to sign a separate document entitled Our Community Health Center Confidentiality Agreement. The term “Employee” refers to all full and part-time employees including but not limited to temporary, contract, volunteer, and student personnel.

300.2.b: Information Management and Telephony Consultants. All external Telephony and Information Systems Consultants may be required to sign a separate document entitled Our Community Health Center Confidentiality Agreement. The term “Telephony and Information Systems Consultants” includes but is not limited to integrators, programmers, hardware and software technicians, telephone system technicians, and Internet carriers, with the exception of circuit providers. The Chief Executive Officer (CEO) or designee may waive this requirement on a vendor by vendor basis.

300.2.c: Financial and Business Consultants. All external Financial and Business Consultants who have the possibility of coming in to contact with any technical, strategic, and marketing plans, financial reports, projections, production figures, capacities, detailed technical information and processes, business and financial information on contracts, supply arrangements, patient volumes, clinical and demographic patient information, information contained in tax returns, or financial statements may be required to sign a separate document entitled Our Community Health Center Confidentiality Agreement. The term “Financial and Business Consultants” includes but is not limited to grant, marketing, strategic, and special project consultants, attorneys, auditors, or any other agency or person that comes into contact with any of the aforementioned information. The Chief Executive Officer (CEO) or designee may waive this requirement on a consultant by consultant basis.

Policy 300.3: Before a OurHealthNet user account can be created for an authorized full or part time employee, temporary employee, contractor, volunteer, student, board member or other personnel an Employee Action Communication Form must be completed by the OurHealthNet user's supervisor.

- There is a two day timeframe for each OurHealthNet user account creation. Insure the form is completed at least 2 days before the action date.
- You can find this form by going to <http://OCHC website>

Policy 300.4: OCHC will require all OurHealthNet users including but not limited to any authorized full or part time employee, temporary employee, contract volunteer, student, board member or other personnel accessing OurHealthNet from either an external or internal console to attend initial computer use, application use, and security training sessions before receiving access codes or passwords to OurHealthNet.

Policy 300.5: New or Current OurHealthNet users are required to complete OurHealthNet training.

- All OurHealthNet users will be required to attend compliance training offered. To signify completion of training, all participants must complete a post-test and sign the attestation of attendance and compliance agreement.
- All new OurHealthNet users will be required to complete the security training sessions within fifteen (15) days of employment. To signify completion of training, all participants must complete the post-test and sign the attestation of completion and compliance agreement.
- Compliance training will be ongoing and continued participation is required. Training may occur in staff meetings, via newsletters, e-mails, bulletin boards, or online.

Policy 300.6: Supervisors must directly notify IT 24 hours before a OurHealthNet user's planned termination or resignation. In the case of an unplanned termination, IT must be directly notified by the end of the day that the termination takes place. An Employee Action Communication form will have to be completed to communicate this termination. Furthermore, it is the responsibility of IT to disable or lockout access to OurHealthNet.

- You can find this form by going to <http://OCHC website>

Our Community Health Center has implemented Virtual Private Networking (VPN) or remote access to allow OurHealthNet users to connect to OurHealthNet from their personal home computer. To have the software installed on your home computer you will need permission from your supervisor. This installation will require you to bring your home computer to the Information Technology Department.

Policy 300.7: Remote access and the installation and continuation of use of OCHC owned software on a OurHealthNet user's home personal computer or laptop will be subject to a separate document entitled "Conditions for installation of Our Community Health Center owned software on a privately owned computer".

Policy 300.8: Any OurHealthNet user who participates or attempts to bypass such practices as outlined in policies 300.1 through 300.7 will be subject to disciplinary action up to and including possible termination of employment. In the case of a non-employed OurHealthNet user, access to OurHealthNet will be locked-out.

A OurHealthNet user is defined as any authorized full or part time employee, temporary employee, contract, volunteer, student, or board member accessing OurHealthNet from either an external or internal console.

User authentication security is defined as any measures utilized to accurately authenticate and identify authorized and unauthorized users of equipment, data, or network systems. It is also defined, for convenience within this manual, as any policy or procedure relating to authenticating and identifying authorized users.

OCHC's User Authentication Security risks are passwords, user accounts, and any other method of accurately authenticating and identifying authorized users. An acceptable User Authentication Security design will prevent unauthorized access from a breach of security originating from easily guessed passwords, password or account sharing, and password or account hacking.

To prevent and counteract account password hacking or cracking OurHealthNet automatically prompts users to change their password after a given duration of days (this process can not be bypassed), further it will not allow users to change their password to one that has been used during the past several changes. OurHealthNet locks out an account after several inaccurate authentication attempts; this lockout exists for a given amount of time.

Policy 301.1: OurHealthNet Systems have a password complexity requirement for all passwords used by OurHealthNet Users:

- Passwords must be at least 6 characters long.
- Passwords may not contain your OurHealthNet user name, any part of your full name, birth date, or social security number. (ie: jsmith000 is not acceptable)
- Passwords must contain characters from at least three of the following four categories:
 - Upper case letters (i.e.: A,B,C,...Z)
 - Lower case letters (i.e.: a,b,c,...z)
 - Numbers (i.e.: 0,1,2,...9)
 - Punctuation marks and other symbols (i.e.: !,@,#,\$,%,...>, etc.)

Policy 301.2: OurHealthNet Voicemail has a password complexity requirement for all passwords used by OurHealthNet Users on all telephone voicemail systems (including office phone voicemail, cell phone voicemail, and all other voicemail telephony systems):

- Passwords must be at least 4 to 6 numerals long
- Passwords must not contain your telephone extension or any part of a Our Community Health Center phone number.
- Passwords must not have more than 2 repeating numbers (i.e.: 1110 or 1111 are not acceptable) and must not have more than 2 numbers in consecutive order (i.e.: 1231, 1234 and 9876 are not acceptable).

Policy 301.3: OurHealthNet automatically requires users to change their passwords at least annually. OurHealthNet will prevent users from using their past 10 (ten) passwords.

Policy 301.4: OCHC will implement systems that automatically lock OurHealthNet user sessions within a maximum 5 minute timeline of inactivity. If this timeline is seen to disrupt efficiency, some other type of authentication method will need to be evaluated (i.e.: proximity or biometrics).

Policy 301.5: OCHC will implement systems that prevent OurHealthNet users from logging on after business hours and during weekends. Exceptions to the policy will only be given on a need by need basis.

- Requests for exceptions will need to be made to the Security Officer at least 2 days ahead by the OurHealthNet user's direct supervisor.

Policy 301.6: OurHealthNet users who use Personal Digital Assistants (PDA) that contain OCHC information must password protect them when not in use.

Policy 301.7: OCHC has implemented systems that lockout accounts after a maximum of 3 (three) inaccurate authentication attempts. This lockout exists for a maximum duration of 1 (one) hour unless overridden by an IT staff member.

Policy 301.8: Passwords that are used to access any OurHealthNet service, device, or computer, whether owned or not owned by Our Community Health Center, that contains Our Community Health Center data falls under the category of "confidential information" as defined in a separate document entitled Our Community Health Center Confidentiality Agreement. As such, OurHealthNet users will not store any of their passwords in any way, other than through memorization. Inappropriate examples of storing passwords are recording a password in a personal notebook, wallet, purse, or posting a password on a monitor, under a keyboard, etc.

Policy 301.9: OurHealthNet users will not divulge their authentication code or password to anyone, including their supervisor, unless requested by an IT staff member or with written permission from IT.

Policy 301.10: Unless prior approved, per each instance by the Security Officer, OurHealthNet users will not divulge any *user name, password, PIN, building alarm code, or other secret code including but not limited to modem telephone numbers and TCP/IP addresses* to any person over a telephone, cell phone, or other telephony device. If any person calls and asks for any of the aforementioned information over a telephone, cellphone, or other telephony device the OurHealthNet user will refer them to call Our Community Health Center's Information Technology Department at (919) 250-2925.

Policy 301.11: All OurHealthNet Users are required to log off of terminals before leaving them unattended for any length of time. At no time is a OurHealthNet user allowed to log on using another OurHealthNet user's password.

Policy 301.12: Under no circumstances may patients, family members, patient representatives or OurHealthNet user family members be allowed to view data in the system or gain access to OurHealthNet.

Policy 301.13: OurHealthNet users will not install software on any OurHealthNet computer, workstation, server or device without expressed permission from an Information Management Department staff member. The only users who are authorized to install software without permission are those employees within the Information Management Departments. Software that was not authorized by the Information Management Department, if found on a OCHC owned computer, will immediately be uninstalled.

Policy 301.14: OurHealthNet users will not install and / or play games on OurHealthNet.

Policy 301.15: OurHealthNet users will not download applications or programs off of the Internet using OurHealthNet. Though it is noted however, the downloading of *data files* (i.e.: PDF files, Word Processing Files, Sound Files, etc.) are not considered applications or programs within this manual.

Policy 301.16: OurHealthNet users will not participate in the use of or install software to be used with file, movie, video, or music sharing networks. Examples of file, movie, video, and music sharing networks are Napster, Kazaa, and Morpheus. If file, movie, video, or music sharing software is found on a OCHC owned computer – the software will immediately be uninstalled.

Policy 301.17: OurHealthNet users will not participate in the use of or install software to be used with any instant messaging or chat service, unless organizationally implemented as an IT service. For instant messaging to be implemented organizationally it must be proven to be secure and auditable. Examples of instant messaging and chat services are AOL Instant Messenger, MSN, ICQ, and IRC. If instant messaging or chat service software is found on a OCHC owned computer – the software will immediately be uninstalled.

Policy 301.18: Unless otherwise approved by the Security Officer, or designee, OurHealthNet users will not transport Our Community Health Center information using any free email service or any third party email account. Examples of free email services are Hotmail, Juno, Yahoo, etc. An example of a third party email account would be your personal home email. The only email services that are available for the transmission of Our Community Health Center information are email services provided to users by Our Community Health Center' Information Technology department. If free or third party email access software is found on a OurHealthNet owned computer – the software will immediately be uninstalled.

Policy 301.19: OurHealthNet users will not email or attach to an email any form of information containing a patient's Name, Address, Date of Birth, Date of Service, Telephone number, Fax number, E-mail address, Social Security Number, Account Number, Certificate / License Number, Vehicle Identification number, photograph, biometric information, or any other type of Protected Health Information.

Policy 301.20: Users of OurHealthNet will not access, cause to be accessed, or create the possibility of accessing any system, equipment, or data that they are not authorized to use.

Policy 301.21: OurHealthNet users will not search for, display, print, create, buy, sell or distribute pornography using any portion of OurHealthNet.

Policy 301.22: OurHealthNet users will not bypass proper identification by logging on to any OurHealthNet system as someone else. OurHealthNet users will not share accounts, in any form.

Policy 301.23: Non-OurHealthNet users will not be allowed access to OurHealthNet.

- Non-OurHealthNet users are defined as any person who does not have access to OurHealthNet or who does not have an individual OurHealthNet account. Examples of non-OurHealthNet users are Drug Reps, vendors, and janitorial staff.

Policy 301.24: OurHealthNet users will not install or connect any type of hardware to any portion of OurHealthNet unless with written permission from the Information Management Department.

Policy 301.25: OurHealthNet users faxing out going documents must use a cover sheet that clearly details a security disclaimer. The cover sheet must not contain any type of Protected Health Information.

- OurHealthNet users will take care to insure faxed documents are only received by the intended recipient(s). Reasonable methods of insuring this are:
 - Double-checking fax numbers
 - Keeping a fax number “cheat sheet” near the fax machine
 - Calling the intended recipient to insure the fax arrived

OCHC licenses the use of computer software from a variety of outside companies. OCHC does not own this software or its related documentation and unless authorized by the software developer, does not have the right to reproduce it except for backup purposes. According to applicable copyright law, persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties

including fines and imprisonment. Any doubts concerning whether any OurHealthNet user may copy or use any given software program should be raised with Information Technologies (IT) before proceeding.

Policy 301.26: OurHealthNet users will use software only in accordance with the license agreements.

Policy 301.27: OurHealthNet users learning of any misuse of software or related documentation are required to notify their supervisor or the IT department immediately.

Our Community Health Center implemented a Helpdesk system to track OurHealthNet user's computer, telephone, cell phone, long-distance, and pager requests. This system was designed to make use of standardized incident subjects (i.e.: E-time, ADP, Medic, Telephone, and Time Clocks). Given the Service Level Agreement (SLA) or priority per each user, center, or standardized support subject, the system emails or messages IT personnel via their cell phones. Automatically based on the SLA is an expected resolution time frame. This resolution time can vary based on workflow and other projects.

Policy 301.28: OurHealthNet users needing to communicate an incident or new request to the Information Management Department will use the Helpdesk system.

- Each new OurHealthNet user will receive an initial training on the proper use of the Helpdesk.
- A OurHealthNet Helpdesk manual can be found online by going to <http://OCHC website>.
- OurHealthNet users may request a paper manual by entering an incident into the helpdesk system.
- If the Helpdesk is unavailable due to a system problem then please contact the computer room by calling *****
 - If no one answers you call, then please contact the Administration front desk by calling ***** x0

Policy 301.29: Any OurHealthNet user who participates or attempts to bypass such practices as outlined in policies 301.1 through 301.28 will be subject to disciplinary action up to and including possible termination of employment. In the case of a non-employed OurHealthNet user, access to OurHealthNet will be locked-out.

302	Security and Risk: Physical Security
-----	--------------------------------------

- OCHC's physical security risks are building security, server rooms, network equipment, and Wide Area Network (WAN) provider connectivity equipment. Physical security begins with locking server and network equipment room doors and having office security systems.

Policy 302.1: Only employed OurHealthNet users shall receive keys, codes, or pass phrases to building alarm systems and perimeter door locks.

Policy 302.2: OurHealthNet users having received keys, codes or pass phrases to building alarm systems and perimeter door locks will not bypass proper identification by swiping or coding in as someone else. OurHealthNet users will not share their building alarm system and perimeter door lock keys, codes, or pass phrases, in any form.

- In the event that an authorized person has forgotten their keys, codes, or pass phrases to a building alarm system or perimeter door lock – they will use the public entrance.

Policy 302.3: Employee only or back door Perimeter door locks must stay locked at all times.

Policy 302.4: Our Community Health Center will make every effort to ensure that there are physical safeguards in place to protect data from inadvertent or illegal access.

- Receipt of any diskettes, tapes or other forms of media that contain Protected Health Information (PHI) will be noted in the OurHealthNet information management inventory. Information will be transferred to the practice system in a timely fashion (within 10 days) and materials used for transmission of information will be destroyed.
- Removal of hardware and software from any OCHC site that might contain protected health information is prohibited.
- OCHC will keep a log of system maintenance procedures and verify the identification of any maintenance personnel not known.
- Workstations will be placed in secure areas where monitors are not easily viewed by patients or unauthorized personnel.
- All visitors to the practice for reasons other than treatment will be asked to sign in and verify their identity before being allowed to enter secure areas.

Policy 302.5: OCHC will physically secure all offices and rooms containing OCHC owned servers and integral switching, routing, Wide Area Network provider connectivity equipment. In addition OCHC will also secure rooms containing corporate consolidated organizational data, information, and knowledge in the electronic form.

Policy 302.6: Only those OurHealthNet users who require day to day access to the areas in policy 302.5 shall receive keys or codes to those secure places.

Policy 302.7: Vendors, consultants, and service providers shall not receive keys or codes to sensitive equipment or data storage areas, without approval from the Security Officer or Designee.

Policy 302.8: OurHealthNet equipment and devices must be positioned within offices such that information can not be seen by non-OurHealthNet users.

- OurHealthNet equipment and devices include but are not limited to computers, monitors, fax machines, copiers, printers, scanners or any other equipment or devices that contain, display, or capture OurHealthNet Information.

Policy 302.9: All personnel will wear their name tag and / or photo ID at all times while on any company premises.

Policy 302.10: Any OurHealthNet user who participates or attempts to bypass such practices as outlined in policies 302.1 through 302.9 will be subject to disciplinary action up to and including possible termination of employment. In the case of a non-employed OurHealthNet user, access will be locked-out.

Network Operating System (NOS) Security is the biggest determining factor of OurHealthNet's security. A NOS is any Operating System (OS) that is network aware. A network is a method of connecting multiple systems together to achieve something greater than its part. An OS is basically any software system that primarily operates a computer. For example, Medic is a database, while IBM AIX (The OS that Medic runs on) is a NOS. Windows NT Server and Workstation or Windows 2000 Server and Professional is a NOS, while natively Disk Operating System (DOS) and Windows 3.1 is nothing more than an OS. DOS, Windows 3.1, 95, and 98 have very little built in security, short of integrating with a Windows 2000 Server. A network can be made up of multiple NOS. Using this cross-platform architecture creates diversity in what and how information can be accessed and integrated. Cross-platform architecture is the method of integrating multiple NOS and applications into a seamless system (i.e.: Misys, Multiview 2000, and MS 2000 Server with Citrix Metaframe).

OCHC's NOS risks are file, directory, and service (i.e.: Internet Firewall) authentication. A secure NOS will protect and prevent internal and external factors from causing data loss, data damage, and unauthorized access. To fully secure an integrated network each part needs to be secured individually – as well as the whole. Each NOS part, from data management to presentation, has to authenticate legitimate users beginning with password level.

OCHC's primary NOS are Windows 2000, AIX, and Linux. OCHC uses Microsoft Windows object and auditing security services. Firewalls provide Internet security on OCHC's internal network and a virus shielding server provides scanning of Web, FTP, POP, and SMTP packets.

Connectivity Security is the security implemented on the transport, data link, and connection portions of a network that prevent unauthorized individuals from interrupting or intercepting data in transport. It also prevents unauthorized users from connecting to or accessing services, devices, and data. *Physical Security* is the physical barriers that prevent unauthorized individuals from gaining access to integral equipment.

OCHC's Connectivity risks are Internet access, Virtual Private Networking (VPN), dial-up, telephone, and Physical Network Link Access. An acceptable connectivity security design will prevent unauthorized access to internal services, equipment, and data originating from a breach in the internal security services of Firewall, VPN, dial-up, telephone, and Physical Network Link Access.

OCHC uses Cisco switches and routers to facilitate OurHealthNet connectivity. Routers and switches are monitored with Cisco View 2000 and Unicenter. Connectivity between sites is achieved through the use of dedicated point to point T1 lines. Unused switch ports are disabled to prevent unauthorized network access. Switches and Routers are password protected. A Watchguard Firebox firewall is used to protect OCHC from Internet attacks. Log entries are generated on a per hit basis. Possible unauthorized Internet penetration is logged. Daily reports are available to authorized personnel.

Policy 1001.1: OCHC will only integrate applications, network operating systems, and technological services that are considered by industry standards to be secure. Those aforementioned integrated components must also be capable of preventing internal and external factors from causing data loss, data damage, and unauthorized access.

Policy 1001.2: OurHealthNet's administrator passwords will be changed on an annual basis and in the event of Senior Management or Information Management Department personnel changes.

Policy 1001.3: Our Community Health Center will manage system integrity by proactively checking for viruses, detecting and containing inadvertent or illegal access, developing an inventory of all hardware and software and correction of any weaknesses in the system.

- The Security Officer or System Administrator will work with vendors to ensure that proper mechanisms are in place to prevent, detect, contain and correct any security breaches.
- These mechanisms will include regular system virus checks, security testing and maintenance review of hardware and software for security breaches as prescribed by the vendor.
- All mechanisms used to manage the security configuration of the system will be documented by the vendor or the Security Officer at regular intervals.
- Any breaches of security detected by the System Administrator or Security Officer will be solved by the Security Officer or discussed with the vendor. Partners of the practice will be informed about security breaches and allowed to comment on solutions designed to respond to them.
- Periodically, security processes will be reviewed and updated by the Security Officer or System Administrator along with the vendor. The Security Officer will conduct an annual risk analysis and devise a plan to manage risk.
- Any OurHealthNet user suspected of intentional involvement in security breaches will be terminated. Any OurHealthNet user that is inadvertently involved in a security breach will be offered training and education on system procedures.
- Periodically, the Security Officer and / or the System Administrator will conduct training sessions for OurHealthNet users to alert them to specific security risks.

Policy 1001.4: OCHC will only integrate connectivity services and equipment that meet or exceed industry-established standards for security.

Policy 1001.5: OCHC will use approved security systems and measures recommended to it by its patient accounting system and other software vendors to protect the integrity, confidentiality and availability of electronic data. OCHC will document its selection of security measures and update its documentation periodically.

- OCHC will inventory all software programs and systems that could contain protected health information.
- Vendors for those software programs will be contacted and asked to provide a diagram and documentation of the security measures and access levels available in the software.
- The Security Officer for the practice will select an appropriate level of security that includes at least the following: individual authentication of users, access controls, audit trails, physical security, disaster recovery, protection of remote access points, protection of external electronic communications and periodic system assessment recommendations.
- Documentation of the selection process and the choice of security system will be kept by the Security Officer. Documentation of system security levels will be made available to individuals responsible for implementation.
- The documentation of the security system and security measures will be updated every three years to ensure that a HIPAA approved level of security is maintained.

Policy 1001.6: The OCHC IT department will internally, conduct security audits on services, connectivity, and systems on a quarterly basis or when any services, connectivity, or systems have been added or modified. Measures will be taken to make improvements in the security system should they be deemed necessary by OCHC.

- The following systems will be audited:
 - Terminal Servers
 - Application Servers
 - Data Servers
 - All Connectivity Devices
 - User Accounts
 - Email Accounts
 - Service Accounts
 - Administrator Accounts

- Firewall Policies
- VPN Accounts
- Virus Protection System

Policy 1001.7: The OCHC IT department through external consulting firms will conduct security audits on services, connectivity, and systems on a three year basis. Measures will be taken to make improvements in the security system should they be deemed necessary by OCHC.

The securing of data, for use in this manual, is defined as any method or methodology of securing stored data in a way that prevents unauthorized access and guarantees its uncorrupted availability in the future.

The risk of data security is who or what has access to that data.

To overcome that risk, OurHealthNet uses a combination of NOS object security, auditing, redundancy, and user account, password based access security, and physical security. OurHealthNet also secures its data through maintaining daily backups and having at least a one-week-old copy off site at all times in a fireproof locked safe. These off site backups are protected and encrypted with a password.

OurHealthNet audits and secures data on per user and per user group basis. In the following example, Mary and John are users on OurHealthNet and IT has created a data directory called “Finance” on a server called “OCHCdata”. Mary is part of a user group called “Finance”, while John is only part of a user group called “Patient Accounting”. IT has given the Finance and Administrative groups access to Finance. In this example, Mary, not John has access to the data directory “Finance”. If John were to try to access Finance (even though he does not have access to it) an audit entry would be created and recorded in the OurHealthNet security database. Each time John tries to access a directory he does not have access to the date, time, machine that he is logged on to, the directory he is trying to access is logged. OurHealthNet also audits the act of copying, moving, deleting, writing and opening certain files. The following file types are fully audited: protected health information, personnel data and salary information, financial data, financial bank access, financial general ledger and financial accounts payable.

Policy 1001.8: OCHC will backup its essential organizational data using industry standard backup media and equipment that allows restoration in the event of a hardware or software failure. Essential organizational data, for the use of these policies, is defined as any data that could be deemed critical to operations or that would take significant time recreating if lost or corrupted.

Policy 1001.9: OCHC will store offsite copies of the media in Policy 1001.8 on a weekly or quarterly basis.

- Copies will be maintained in a safety deposit box.

The storing of data, for the use of this manual, is defined as any method or methodology of storing information or knowledge for immediate or future use in a way that guarantees that data’s accessibility immediately or in the future.

The risk of data storage is how and where that data is stored.

To overcome that risk OCHC uses a mixture of redundancy and Redundant Array of Inexpensive Disks - Five (RAID-5) storage. Depending on the particular situation, the data will either be redundant or stored within a RAID-5 Array. The other two alternatives are that the data can be very easily recreated such that it has no need to have any particular secured storing methodology, or that the system housing the data has no way of providing Redundancy or RAID-5 storage.

Policy 1001.10: OCHC will ensure data is stored in a secure place using redundancy, RAID-5 storage, or some other industry acceptable mean of securely storing data that gives the same effect.

Data presentation, for use in this manual, is defined as any method or methodology of displaying or transmitting OurHealthNet data.

The risk of data presentation is how OurHealthNet data is transmitted and displayed.

To overcome that risk, OCHC uses encryption technologies when appropriate during transmission through areas that are not contained or controlled by OurHealthNet. Examples of such situations requiring encryption are when a OurHealthNet user uses VPN technologies or connects to a OurHealthNet Terminal Server from a dial-up or VPN connection.

Policy 1001.11: Unless encrypted or deemed by computer industry standards to be secure, OCHC will not implement wireless networking.

Policy 1001.12: OurHealthNet will use encryption technologies when transmitting OurHealthNet data through areas not contained or controlled by OurHealthNet.

- Our Community Health Center will instigate integrity controls and message authentication. Internal networking can be considered secure as long as a user based security system where all users have a specific identification and access code is used.
- If Our Community Health Center uses the Internet to transmit data, some form of encryption device will have to be employed.
- Value added networks, private wires and dial up connections are not subject to the encryption requirement.
- If the vendor's software offers integrity controls and message authentication Our Community Health Center will take advantage of those.

Policy 1001.13: Access to OurHealthNet information will be restricted to those OurHealthNet users who have a business need to use it.

- The Security Officer and Information Management Department will have emergency access to the system. All other types of access to the system will be restricted based on the contextual use of the information (e.g.: insurance department will have access to all data necessary to process and mail out claims); the role of the user (e.g.: therapists will have access to chart notes and medical records but not necessarily insurance information) and/or the type of user (e.g.: some users will be able to view and change data in certain areas of the system while others will only be able to view it or may not be able to see it at all).
- All OurHealthNet users must be given clearance by the Security Officer prior to accessing the system. In order to gain security clearance, the OurHealthNet user must have an active position that requires system access. Persons that do not require system access (Janitors etc) will not be given passwords or access to the system.
- Once access is defined, the Security Officer or designee will assign all OurHealthNet users individually identifiable passwords. All OurHealthNet users will be required to log in to the system using their unique password and the system will log OurHealthNet users off after a specified period of time in which there has been no input from the user.
- The Security Officer or System Administrator will be responsible for maintaining and managing levels of access and user passwords. OurHealthNet users will be required to maintain the confidentiality of their passwords.
- Monthly or at least quarterly, the System Administrator or Security Officer will run reports to audit system access. Other mechanisms may be put in place to monitor system access from entry points other than user entry.
- Security incidents will be noted and logged. The System Administrator or Security Officer and vendors or security specialists will address any security breaches.
- Routine changes to system hardware and software will be validated against the security system to avoid creating inadvertent security weaknesses.

Policy 1001.14: The IT Department will test all security and backup systems quarterly to ensure that they are operating properly.

10000 | OurHealthNet: Contingency plans for responding to system emergencies

OCHC's risks for System Emergencies are Virus Outbreak, System and Network Intrusions, Site to Site Circuit Loss, Data Loss, Fire, and Power Loss.

Policy 10000.1: OCHC will develop and follow a contingency plan for backup and storage of data to allow for recovery of OurHealthNet in the event that the system or network is compromised.

- With input from senior management the IT department will prioritize all software applications and services based on its criticality of data. This will allow priority to be identified when implementing contingencies during System Emergencies.

- In the event of a Virus Outbreak:
 1. Cut off access to the infected portion or portions of the network up to and including disconnection from the internet and/or internal sites.
 2. Cut off access to the infected system or systems
 3. Notify Senior Management and Managers
 4. If possible, identify who initiated the virus outbreak
 5. Identify how and where and when the virus outbreak took place
 6. Run virus protection systems
 7. Implement Safeguards to prevent future infections
 8. Delete all suspect data and restore from backup
 9. Test
 10. Open back access to the affected system or systems
 11. Notify Senior Management and Managers
 12. Open back access to the affected portion or portions of the network.
 13. Input Incident into Helpdesk
 14. Test

- In the event of a System or Network Intrusion:
 1. Cut off access to the affected portion or portions of the network up to and including disconnection from the internet and/or internal sites.
 2. Cut off access to the affected system or systems
 3. Notify Senior Management and Managers
 4. If possible, identify who initiated the intrusion
 5. Identify how and where and when the intrusion took place
 6. Implement Safeguards to prevent future intrusions
 7. Delete all suspect data and restore from backup
 8. Test
 9. Open back access to the affected system or systems
 10. Notify Senior Management and Managers
 11. Open back access to the affected portion or portions of the network.
 12. Input Incident into Helpdesk
 13. Test

- In the event of Site to Site Circuit Loss:
 1. Diagnose the Circuit
 2. Identify Issue
 - Notify Senior Management and Managers
 - If Internal Issue
 - Solve problem
 - If Circuit Provider issue
 - Contact Circuit Provider to open incident
 3. Once service is restored, Test

4. Notify Senior Management and Managers
 5. Input incident into Helpdesk
 6. Continue to run tests on circuit for 24-48 hours
- In the event of Data Loss:
 1. Identify what data was lost
 2. Notify Senior Management and Managers
 3. Identify what caused data loss
 4. Solve issue or replace failing component
 5. Test
 6. Restore Data if required
 7. Bring online system that experienced loss of data
 8. Notify Senior Management and Managers
 9. Input Incident into Helpdesk
 10. Test
 - In the event of Fire Loss:
 1. Locate data Backups
 2. Notify Senior Management and Managers
 3. Find and test replacements for integral equipment that was lost
 4. Test Backups
 5. Restore Data
 6. Input Incident into Helpdesk
 7. Test

Policy 10000.2: OCHC will implement power backup for all systems that are integral to the processing of Our Community Health Center Information.

- In the event of Power Loss:
 1. Shutdown Systems affected by power loss
 2. Shutdown Battery Backup serving systems affected by power loss
 3. Notify Senior Management and Managers
 4. Identify reason for power loss
 - If Internal issue
 - Solve problem or contact facility management
 - If Power Company issue
 - Call Power Company
 5. Once power is restored, Test
 6. Notify Senior Management and Managers
 7. Wait 10-15 minutes
 8. Bring back up Battery Backup serving systems affected by power loss
 9. Bring backup Systems affected by power loss
 10. Input Incident into Helpdesk
 11. Test