Quality Systems, Inc

Privacy Policy Handbook

(March 2003)

TABLE OF CONTENTS

A. Overview.....3
B. HIPAA 3
Definitions
Covered Entity.....5
Incidental Use & Disclosure.....5
Minimum Necessary.....6
Business Associate.....6
Protected Health Information.....7
Individually Identifiable Health Information.....7
C. Internal Policies.....8
Access Control.....8
Anti-Virus Protection 9
Avoid Inappropriate Content And Behavior 9
Backup & Recovery 11
Business Associates Non-Disclosure Agreements 12
Customer Databases 12
Company Documents 13
E-Mails.....14
Handling and Destruction of Confidential Information.....15
Passwords.....19
Personnel 18
"Chief Privacy Officer" 18
Network Administrator 18
Information Owners 19
Department Managers.....20
Information Users.....20
Physical Access Control.....20
Remote Access/Users 21
Use of the Internet 21
Violation Reporting & Corrective Action 22

A. Overview{ XE "A. Overview" }

Why a Privacy Policy? While the Company (Quality Systems, Inc.) has always had policies protecting its and its customer's confidential information, two factors have moved us to more formally document our policies: (1) new healthcare regulations (HIPAA) and (2) the growth in the size of the Company.

The purpose of this policy is to assist our staff members in balancing their need for securing and protecting both the Company's and our customer's confidential information and their need to perform their duties.

As you would expect, changes to this policy are inevitable and we'll benefit from your feedback (and our customer's feedback) to assist us in making this policy both protective as well as practical.

B. HIPAA{ XE "B. HIPAA" }

The Health Insurance Portability and Accountability Act ("HIPAA) is a comprehensive set of new Federal regulations that effect the healthcare industry. The key section impacting our Company is the Administrative Simplification section, which includes, among other sections, the rules and regulations involving: (i) Transaction and Code Set standards, (ii) Privacy and (iii) Security.

The HIPAA regulation applies directly only to 'covered entities', which is a defined term under the regulation, but generally, includes all of our customers. The Company is potentially a "covered entity" (herein after in this document Company will be referred to as a "covered entity") and hence prudently we should observe the HIPAA regulations.

Because HIPAA impacts the Company and our clients, it affects the role our product(s) play in helping to facilitate our client's compliance with their regulatory obligations. But, our involvement with HIPAA extends beyond this.

Under HIPAA, any covered entity that will be working with a third party, who may have access to patient identification information, ***must*** enter into a Business Associates Agreement with such third parties. Because we come into contact with protected patient information in our training, installation and support of the Company's software, our customers may require us to enter into a Business Associate Agreements with them. And, because, at times, we may need the assistance of our third party partners in solving a customer's needs, we may need to enter into a Business Associate Agreement with our third party partners. These Business Associates Agreements contractually bind the Company (and any of our third party vendors who sign a BAA) to those applicable portions of the HIPAA regulations outlined in the Business Associates Agreement.

While the Security regulations have not yet been finalized, the Privacy rule does include references to 'security' and our Privacy policy is a mixture of privacy and security rules. However, before you can understand the rules, you'll need a quick

overview of the HIPAA Privacy rule and an understanding of some key terms under the Rule.

The Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164) provides the first comprehensive Federal protection for the privacy of health information. (However, more restrictive State privacy rules, if they exist, may take precedent over the HIPAA regulations.) The Privacy Rule, as modified, is carefully balanced to provide strong privacy protections that do not interfere with patient access to, or the quality of, health care delivery.

By the compliance date of April 14, 2003 (April 14, 2004, for small health plans), covered entities must implement standards to protect and guard against the misuse of individually identifiable health information. Failure to timely implement these standards may, under certain circumstances, trigger the imposition of civil or criminal penalties.

The HIPAA Privacy Rule for the first time creates national standards to protect individuals' medical records and other personal health information.

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights
- And it strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.

For patients – it means being able to make informed choices when seeking care and reimbursement for care, based on how personal health information may be used.

- It enables patients to find out how their information may be used, and about certain disclosures of their information that have been made.
- It generally limits release of information to the minimum reasonably necessary for the purpose of the disclosure.
- It generally gives patients the right to examine and obtain a copy of their own health records and request corrections.
- It empowers individuals to control certain uses and disclosures of their health information.

With this background, what follows are a set of guidelines for each of us to follow in an effort to keep disclosure of confidential information to a minimum. We will need for each of you to think carefully when you come into direct or indirect contact with confidential information. The guiding principle is that you should not disclose any confidential information to any non-employee without a written authorization from the customer to do otherwise and you should restrict its disclosure to only those

employees that you need to help you achieve your task. If enforcing this principle interferes with your doing your job, bring this fact to the attention of your manager, who will guide you accordingly.

Definitions{ XE "Definitions" }

To assist you in understanding the scope and application of this privacy policy, it is important that you understand key HIPAA-defined terms used throughout this document, in particular:

1. Covered Entity{ XE "Covered Entity" }

   Under HIPAA, this is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction.

2. Incidental Uses and Disclosures{ XE "Incidental Uses and Disclosures" }

   In summary, it is not expected that the privacy of protected health information is guaranteed protected from any and all potential risks. Rather, it aims to achieve a level of reasonableness in protecting individuals' health information – for instance:

   By speaking quietly when discussing confidential information (including any patient information used by you in performing your duties) in public area;

   By avoiding, when possible, using or accessing real patients' information in any training or support situation.

   By isolating or locking file cabinets or keeping customer's information in separate folders; or

   By providing additional security, such as passwords, on computers maintaining private company and/or customer information.

   Remember, protection of patient confidentiality is an important practice for our customers; and, we should seek to abide by the reasonable privacy policies of our customers and the rules of common sense at all times.

   Our customers also must implement reasonable minimum necessary policies and procedures that limit how much protected health information is used, disclosed, and requested for certain purposes. These minimum necessary policies and procedures also reasonably must limit who within the entity has access to protected health information, and under what conditions, based on job responsibilities and the nature of the business. In turn, we too need to limit our disclosure of any customer confidential information solely to those within our Company who absolutely need such information to perform their job.

3. Minimum Necessary{ XE "Minimum Necessary" }

The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.

The implementation specifications for this provision require a covered entity to develop and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce. While guidance cannot anticipate every question or factual application of the minimum necessary standard to each specific industry context, the covered entity and our Company will be continuing to monitor and codify its findings of this issue in the future.

4. Business Associates{ XE "Business Associates" }

As stated earlier, by law, the HIPAA Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers. However, most covered entities do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule allows covered entities to disclose protected health information to these "business associates" if the covered entities obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule. Covered entities may disclose protected health information to an entity in its role as a business associate *only* to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.

The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

5. Protected Health Information{ XE "Protected Health Information" } ("PHI")
Individually Identifiable Health Information ("{ XE "Individually Identifiable Health Information (\"" }IIHI")

Central to the HIPAA Privacy Rule is the restriction on a covered entity and/or business associates release of PHI. Protected Health Information is all individually identifiable health information ("IIHI") transmitted or maintained by a covered entity, regardless of form. IIHI is a subset of PHI, including demographic information collected from an individual that is created or received by a covered entity or employer and relates to the past, present or future physical or mental health or condition of an individual, or the past, present or future payment for the provision of health care to an individual which identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

The regulation specifically lists 19 key identifiers that would render information IIHI. The 19 identifiers are:

1. Name
2. All address information
3. E-mail addresses
4. Dates (except years)
5. Social Security numbers
6. Medical records numbers
7. Health plan beneficiary numbers
8. Account numbers
9. Certificate numbers
10. License numbers
11. Vehicle identifiers
12. Facial photographs
13. Telephone numbers
14. Device identifiers
15. URLs
16. IP addresses
17. Biometric identifiers
18. Zip codes
19. Any other unique identifying number, characteristic.

Each employee involved in the training, installation and support of our software must keep these identifiers in mind when performing their corporate duties for a customer. When dealing with this type of information, you must pay particular attention to avoiding the disclosure of the materials containing these identifiers.

C. Internal Policies{ XE "C. Internal Policies" }

In your use of the computer system (i.e. your laptop, your desktop and/or the network) employees must comply with all software licenses; copyrights; and all other state, federal and international laws governing intellectual property and online activities.

The computer system is the property of Company and should be used for legitimate business purposes. Users are permitted access to the computer system to assist

them in the performance of their jobs. All users have the responsibility to use computer resources in a professional, ethical and lawful manner. At all times, users have the responsibility to use computer resources in a professional, ethical and lawful manner. Use of the computer system is a privilege that may be revoked at any time.

Each user is responsible for ensuring that his or her use of outside computers and networks, such as the Internet, does not compromise the security of the Company's computer network. This duty includes taking reasonable precautions (many of which are outlined in this manual) to prevent intruders from accessing the Company's network without authorization and to prevent introduction and spread of viruses.

Access Control{ XE "Access Control" }

Your manager initiates the access control approval process. Events, including but not limited to job termination and/or change of duties, may trigger a change in the privileges granted to You. If such an event occurs, your manager must immediately notify the Network Administrator. The existence of certain access privileges does not, in and of itself, mean that you are authorized to use these privileges. If you have any questions about access control privileges, you should contact your immediate supervisor and/or the Network Administrator.

All non-employees (contractors, consultants, temporaries, outsourcing firms, etc.) must also go through a similar access control request and authorization process initiated by the project manager. The privileges of non-employees must be immediately revoked by the Network Administrator upon notification of the project's completion or when the non-employee stops working with the Company.

The Network Administrator is responsible for maintaining a log of files accessed and log-ins attempted by user. If unauthorized system entry attempts occur, the Network Administrator will report these events to the Manager of the Tech Department and/or the VP of Operations at the earliest possible opportunity.

The Network Administrator will audit the following items:

- Unsuccessful network logins greater than three attempts
- Successful and unsuccessful system access
- Firewall penetration attempts

The Network Administrator will notify the Manager of the Tech Department and/or the VP of Operations of any unauthorized attempts to gain access to the LAN, individual workstations, or Confidential Information through any means including local area network connections, wide area network connections, or remote access. Upon discovery of an attempted compromise, the Network Administrator will initiate a report as soon as possible and by no later than the start of the first working day following discovery. Should an actual compromise occur, the Network Administrator would notify the Manager of the Tech Department and/or the VP of Operations as soon as possible.

In order to secure Company information, including any PHI and IIHI, it is necessary to control access to such material that is stored anywhere on the network. You will only be granted access and privileges on Company's systems and/or network servers that are consistent with and necessary for the fulfillment of your job responsibilities.

Anti-Virus Protection{ XE "Anti-Virus Protection" }

Viruses can cause substantial damage to computer systems. To circumvent this, the Company has a dedicated anti-virus protection server that protects the authorized servers, laptops and desktops on the Company's domain. This server gets updated virus definitions from the anti-virus software vendor as they become available. This server then pushes the updates to servers elsewhere in the organization and updates your computer when you log on, whether by a hardwire, wireless, VPN or RAS connection.

However, it is ultimately your responsibility to make sure that precautions are taken to avoid introducing viruses through your computer system into the Company's network.

To that end, all material received on floppy disk or other magnetic or optical media and all material downloaded from the internet or from computers or networks that do not belong to the Company MUST be scanned for viruses and other destructive programs before being placed onto our computer system. You should understand that your home computers and laptops might contain viruses. All disks transferred from these computers to the Company's network MUST be scanned for viruses.

No one other than Network Administrator is authorized to turn off or disable virus-checking systems.

Avoid Inappropriate Content And Behavior{ XE "Avoid Inappropriate Content And Behavior" }

Authorized use of the computer system is solely for the purposes of the Company. While accessing and using the computer system, you may not, for any reason whatsoever,

- perform any act, which constitutes illegal or unacceptable behavior.
- use someone else's access code or password to access the computer system.
- attempt to gain any type of access to information or systems for which you are not authorized.
- use a work station other than your own to access the computer system, unless pre-approved by your supervisor.
- reveal any access code or password to a third party.
- create, install, transfer, download or use computer files that have no relevance to the Company operations.

- create, install, transfer or download, files or software containing viruses, or files or software dangerous to the integrity of computer system.

- engage in software pirating, including the exchange of pirated software.

- connect any equipment or accessory to the computer system without permission of the Company.

- publish, transmit, download, send, print, copy, exchange or store digital information, opinions or documents which are discriminatory, abusive, malicious, threatening, hateful, violent, slanderous, defamatory, fraudulent, racist, sexist, sexual, obscene, or illegal.

- access the computer system and use it for personal, political, or charitable soliciting, or commercial purposes.

- reverse engineer or copy licensed software unless the license agreement specifically provides for it and you have obtained your supervisor's permission. Under no circumstances should the company's proprietary software be reverse engineered or copied.

- load or use copyrighted software on systems for which it is not licensed. This includes employee-owned home computers and other personal digital devices used for the Company.

- license or download any material for which a registration fee is charged without first obtaining the express written permission of your supervisor.

You shall:

- Use the computer system in a prudent and conscientious manner

- Protect the equipment from any object or substance which may hinder its proper operation

- Respect the access and use conventions of the internal and external networks

- Maintain the confidentiality of the access code or password providing access to the computer

- Protect the integrity and confidentiality of the information/data maintained on the computer system, especially any PHI or IIHI used by you in the performance of your duties. This includes the transmission of such information internally from one computer to another.

- Respect and protect the confidential nature of any information transmitted or obtained from the computer system; the method used to transmit information outside the Company depends upon the information's sensitivity, technical risks and threats, external regulations and available communication security controls.

- Enable and disable any modem used by you and supervise its use. Modems should not be left unattended in 'answer' mode.

- Only install or use encryption software on any of the Company's computers after first obtaining written permission from theVP of Operations.

Computer crimes violate state and federal law. They include but are not limited to: unauthorized disclosure, modification or destruction of data, programs, or hardware; denial of computer services; theft of computer services; illegal copying of software; invasion of privacy theft of hardware, software, peripherals, data, or printouts; misuse of communication networks; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under state or federal law, held civilly liable for their actions, or both. Further, such individuals will face disciplinary action by the company up to and including termination.

The federal government has imposed restrictions on export of programs or files containing encryption technology (such as e-mail programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology is not to be placed on the Internet or transmitted in any way outside the United States without the prior written authorization from the President of the Company.

You should not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, subscribing to non-business-related listservers and mailing lists, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents or otherwise creating unnecessary network traffic.

Backup & Recovery{ XE "Backup & Recovery" }

For in house system backups, the Company uses the following backup methodology:

System	Frequency	Storage
QSImain (J30)	Daily (M-F)	Friday stored off site, series of 8
	Monthly (near first of month)	Most recent stored of site, not overwritten
QUIC	Daily (M-F)	Stored in house, series of 8 sets
	Monday night archived and not rewritten	
QSInet	Daily (M-F)	Stored off site
	Monthly (at month end close)	Stored off site (not written over)
Accounting NT	Daily (M-F), series of 4 sets	Stored in house, Wednesdays stored off site
Production NT	Daily (M-F), series of 4 sets	Stored in house, Wednesdays stored

		off site
Mailserver	Weekly, 2 sets	Stored off site

Business Associates Agreements and Non-Disclosure Agreements{ XE "Business Associates Agreements and Non-Disclosure Agreements" }

Before Company releases any confidential information to any third party, that party must first execute Company's Non-Disclosure Agreement. All NDAs are created, distributed and tracked by the legal department. When a Confidentiality Agreement or Non-Disclosure Agreement is requested for a matter, you should send, via e-mail, the following information in your request:

1. the name of the third party entity to whom you desire to send confidential information;
2. the information you desire to provide.
3. the purpose for the release of such information
4. an e-mail address for whom the NDA should be sent.

The VP of Operations will notify You once the signed NDA or Confidentiality Agreement has been received.

Because the Company will be in contact with PHI and/or IIHI in the performance of its training, installation and support of the Company's software, the Company will be requested to sign, and/or may request its third party vendors to sign, a Business Associates Agreement. Whenever possible, Company requires all third party customers and/or vendors to execute its Business Associates Agreement.

The VP of Operations, Executive VP, or President of the Company may only sign any third party Business Associate Agreement.

Customer Databases{ XE "Customer Databases" }

Whenever possible, you should endeavor to use the test patient data in any customer's system to perform your installation, training and/or support duties. Remember, as best you can, try to avoid accessing and/or using any real PHI and/or IIHI data.

If you require a copy of a customer's backup or database for the performance of your duties, you must open a ,HELP regarding same and direct the customer to send, on a tape, a copy of their database directly to your Supervisor. Your Supervisor will then notify you that the database has arrived. When you are ready to work with that database, the Supervisor will release the database to the Database Administrator, who will restore the database. You may then work on the database. Upon completion of the HELP, the Supervisor will then notify the Database Administrator to permanently delete the data from the QSI systems. The Supervisor will return the tape to the customer. No additional copies (either electronic or hard copy) of the database may be made without the written permission of both the customer AND the VP of Operations.

If You work within the Implementation Department, when on site at a customer's location you should avoid hooking your laptop into the customer's network for performing any training. Rather, you should request that the customer make a desktop

system available to you. You should also remind the customer that they should limit your access to their network to solely the files you will need to perform your duties for the customer. This will avoid the possibility of either party needlessly accessing the other's confidential information, as well as avoiding any virus contamination. If training is to be performed at Company's training facility, then customer shall send, if needed, a copy of their database to Network Administrator, who will prepare the database for use on the training room server/network. The trainer will return the original database tape to the customer at the commencement of the training session. Upon the completion of the training session (which could be after multiple days), the trainer will notify Network Administrator of completion of the training and approve the elimination of the database from the training server/network.

Customer Log in{ XE "**Customer Log in**" **}**

Copies of the customer login information "P.CLI" are accessible to authorized personnel to allow them to service the customer remotely. P.CLI resides on a shared volume on the main system. Since you may need to keep some of this information available on your laptop and/or PDA to effectively perform your duties, great care must be taken to keep such information in a password-protected folder.

This information is *strictly* confidential and may only be used for the performance of your duties with the Company. Use by you for any other purposes shall be grounds for immediate termination as well as may lead to criminal and civil charges being brought against you.

Only specific QSI employees by department are authorized to access a client's system, and then only in performance of their QSI duties. Such employees include Developers, Installers, Support Personnel, Marketing Personnel, QUIC/QSINet Personnel, Client Managers, Trainers, Conversion Personnel, and other QSI employees as delineated by client/QSI contracts and/or agreements.

Company Documents{ XE "QSI Documents" }

The VP of Operations & Legal will meet with each department manager to review the suite of forms used by their department in the performance of their team's duties with an eye towards including additional awareness/control over the use of confidential information, including, but not limited to, PHI/IIHI.

Electronic, Fax and/or Hard copy of Confidential Information{ XE "**Electronic, Fax and/or Hard copy of Confidential Information**" **}**

As a general rule, whenever possible, sending or receiving of a fax containing confidential information should be kept to a minimum unless you will be personally faxing (or awaiting the fax) from the machine and will be safeguarding the document during its transmission or receipt. Great care should be taken to avoid having confidential faxes remaining unattended at a fax machine. Always include a cover sheet for any faxes you send, and verify the recipient information prior to sending. The Company has placed various fax machines in closer proximity to each department's work area. You are urged to have any hard copy of a fax be sent to your department's (or the closest fax to your department) fax machine. This will minimize any 'lag time' that a fax may sit at a fax machine.

E-Mails{ XE "E-Mails" }

The Company owns the e-mail service. You cannot expect absolute confidentiality as the Company does, from time-to-time, monitor, observe, view, display and/or reproduce e-mails.

E-mail may be considered official Company correspondence, and you must avoid the inclusion of inappropriate or derogatory language in your messages. E-mail is maintained in computer systems and on backup media for varying lengths of time and may be recovered subsequent to deletion.

Work-related mail is forwarded to the most appropriate employee in the case of employment termination or when an employee is absent for an extended period of time. A recipient may designate another employee to receive and read work-related mail for business reasons. When possible, personal messages are forwarded to the intended recipient. If that is not possible, they are destroyed. The goal is for messages not to be examined further than is necessary to determine the category into which they fall.

Company provides e-mail to its employees to assist and facilitate business communications and work-related research. These services are for legitimate business use only in the course of the employee's assigned duties.

While accessing and using the e-mail system, you may not, for any reason whatsoever,

- Engage in any act that constitutes illegal or unacceptable behavior.
- use someone else's code or password to access the e-mail system.
- allow or tolerate access to the e-mail system or its use by unauthorized persons.
- participate in letter chains, pyramid systems, gambling or computer games.
- lead to believe, through signature of messages or otherwise, that expressing an opinion is on behalf of the company unless authorized to do so.
- represent yourself to a third party as another person.
- copy, transfer or store computer data or files without permission.
- harass a person or group of persons.
- use impolite, abusive or offensive language.
- send information, opinions or documents (e.g.: text, images, audio, video, etc.) which can be construed as discriminatory, abusive, malicious, threatening, hateful, violent, slanderous, defamatory, fraudulent, racist, sexist, sexual, obscene, immoral or illegal.

- knowingly propagate e-mail viruses to other systems.

- automatically forward mail outside of the entity.

- send confidential, proprietary or trade secret information without first obtaining authorization from your supervisor. And, even with authorization, You may not forward such information onto any third party who does not need such information to assist You in the performance of your job.

This footer should be appended to all confidential e-mails sent outside the Company on Company business:

> ***This e-mail, including attachments, may include confidential and/or proprietary information, and may be used only by the person or entity to which it is addressed. If the reader of this e-mail is not the intended recipient or his or her authorized agent, the reader is hereby notified that any dissemination, distribution or copying of this e-mail is prohibited. If you have received this e-mail in error, please notify the sender by replying to this message and delete this e-mail immediately.***

Company's computers that run e-mail routing applications: (1) support and employ security functions such as authentication and logging at the system and e-mail application administrative levels and (2) run on operating systems capable of identification, authentication and other security functions such as logging and discretionary access controls.

Administrators must actively manage e-mail hosts to minimize security risk. System administrators will actively monitor authoritative security sources, perform risk assessments and employ available countermeasures as risks and threats are identified. Specific security guidance includes:

- Hosts should preferably run the most current version of e-mail routing applications. Minimally, the routing software used must incorporate applicable security patches.

- E-mail gateways/mailers must not automatically execute attachments or message bodies, such as those found in Multipurpose Internet Mail Extensions (MIME), ActiveX, SML or Java.

Handling and Destruction of Confidential Information{ XE "Handling and Destruction of Confidential Information" }

You should never request the original version of any confidential information from a customer. Rather, You should solely request a copy of such information.

Printed versions (hardcopy) of *confidential* information should not be copied indiscriminately or left unattended and open to compromise. Hard copies of any customer information that contains confidential information, including but not limited to PHI and/or IIHI, should be kept in folders and secured in a locked file cabinet. At all times, when You are working with such materials on your desk, You should turn such materials over and/or re-file such materials, before you leave your working area – even on a temporary basis.

Media containing *confidential* information should be placed in confidential envelopes and hand-carried by employees or sent through an approved outside carrier. These outside carriers may include, but are not limited to, the U.S. Postal Service, Federal Express and the United Parcel Service.

Magnetic media containing *internal* or *confidential* information, including any database received from a customer, that is released from the Company must first be sent to Support or Development to have such media processed to purge any internal or confidential information residing on that media. Degaussing and overwriting are acceptable methods of purging information from magnetic media.

Responsible personnel should authorize the shipping and receiving of magnetic media and maintain appropriate records.

- When You are finished using any materials that contain any confidential information, including but not limited to any patient or individually identifiable information, You must dispose of the materials in the recycle or trash receptacles.

If you are at a customer's site:

- Before leaving each day, all materials must either be returned to the customer or placed in a secured location approved by the customer. No materials should be taken off-site without the customer's written approval.

Passwords{ XE "**Passwords**" **}**

Users are responsible for safeguarding their passwords for access to the computer resources. All passwords are to be treated as sensitive, Confidential Company information. Individual passwords should not be printed, stored online or given to others – except that an employee may be required to provide management and/or the network administrator with their password. Users are responsible for all transactions made using their passwords (except for any transactions made by management and/or the network administrator using that user's password.) Users may not disguise their identity while using the computer system.

Do not use the same password for Company accounts as for other non-Company access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Company access needs. For example, select one password for log in and a separate password foremail or MAS 200.

Here is a list of "don'ts" when dealing with any password:

- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation (If someone demands a password, refer them to this document or have them speak with your manager or the network administrator.)
- Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every three months.

If an account or password is suspected of being compromised, report the incident to the network administrator and your manager ASAP and change all passwords.

Passwords should be obscure and a minimum of six characters in length. For best security, passwords should include both upper and lower case and special characters (e.g. "@", "!", "&", "%".) Users who do not change their passwords within the time prescribed may be automatically locked out of the system.

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a monthly basis. New passwords shall be distributed by (NETWORK ADMINISTRATOR), via e-mail or orally, to each Manager, who will then distribute the their team, as needed.
- All production system-level passwords must be part of the Company administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every quarterly.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

Everyone should be aware of how to select strong passwords:

Poor, weak passwords have the following characteristics:

- The password contains less than six characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Company", "password" or such other generic phrase.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least six alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that You should have an expectation of privacy in the material You create or receive on the computer system. The Company has a right to inspect, without prior notice, all material stored on its computer system.

Personnel{ XE "Personnel" }

Each employee of the Company shall execute the Company's standard confidentiality agreement upon their hire. In addition, as part of each employee's initial training with the Company, each such employee will receive "Privacy and Security Awareness" training, which will result in their execution of a compliance certification.

The hierarchy of information security responsibility at COMPANY features the following structure:

Chief Privacy Officer
Network Administrator
Information Owners
Department Managers
Information Users

"Chief Privacy Officer"
The "Chief Privacy Officer" is one of the responsibilities of the VP of Operations . In this role, the CPO is responsible for maintaining the privacy of Company and customer data. The CPO should effectively coordinate the development, implementation, and maintenance of a corporate privacy strategy as well as manage the implementation of such privacy programs and revise practices and procedures accordingly. Due to the primary importance of data to operations, each department must be accountable for maintaining the privacy policy and communicating with the CPO.

Network Administrator
The Network Administrator is the central point of contact for all information security matters at COMPANY. Acting as an internal technical consultant, this person is responsible for creating workable information security compromises that take into

consideration the needs of various employees juxtaposed against the threat of security breaches. Reflecting these compromises, the Network Administrator recommends information security standards, procedures, policies, and other requirements applicable to the entire organization to the Chief Privacy Officer. The Network Administrator is responsible for handling all access control administration activities and monitoring the security of Company's information systems.

The Network Administrator is also responsible for providing the Chief Privacy Officer with regular reports about the current state of information security at COMPANY. The Network Administrator will provide technical consulting assistance related to emergency response procedures and disaster recovery. The Network Administrator is also responsible for organizing a response team to promptly respond to virus infections, hacker break-ins, system outages, and similar security problems.

Information Owners

Director level managers are designated as the Owners of all types of information used for regular business activities. In other words, each type of "production system information" needs an Owner. When information Owners are not clearly implied by organizational design, the Chief Privacy Officer will recommend a designation to the CEO. Information Owners do not legally own the information in question; instead, they are members of the COMPANY management team who make decisions on behalf of the firm. Information Owners or their delegates are required to make the following decisions and perform the following activities:

- Approve information-oriented access control privileges for specific job profiles,
- Approve information-oriented access control requests which do not fall within the purview of existing job profiles,
- Select a data retention period for their information, relying on advice from the Legal Department and in compliance with the Privacy Final Rule,
- Select special controls needed to protect information (such as additional input validation checks or more frequent back-up procedures),
- Make recommendations to the Chief Privacy Office and senior management for any new or different uses of their information,
- Review and submit reports of system intrusions and other events which are relevant to their information to the Chief Privacy Officer immediately upon discovery of the event or at the start of the next business day,
- Review and submit reports which indicate the current production uses of their information to the Chief Privacy Officer annually or whenever a change occurs,
- Review and submit reports, which indicate the job profiles that currently have access to their information to the Chief Privacy Officer annually or whenever a change occurs.

Information Owners must designate a back-up person to act if they are absent or unavailable. Owners may not delegate ownership responsibilities to third party organizations (such as outsourcing firms) or to any individual who is not a full-time COMPANY employee. When both the Owner and the back-up Owner are unavailable,

the Vice President in charge of the department may make Owner decisions in question.

Department Managers
Your immediate manager approves a request for system access based on your existing job duties. Similarly, when You leave COMPANY, it is your immediate manager's responsibility to promptly inform the Network Administrator that your privileges must be revoked. User-IDs are specific to individuals and must not be reassigned to or used by others. Within 30 days of separation from COMPANY, the manager is additionally responsible for reassigning the involved duties and files to other staff and informing the NETWORK ADMINISTRATOR of the reassignment.

Information Users
Users are not specifically designated, but are broadly defined as any worker with access to internal information or internal information systems. Users are required to abide by all security requirements. Users are required to familiarize themselves with, and act in accordance with, all COMPANY information security requirements. Users are also required to participate in information security training and awareness efforts. Users must request access from their immediate manager and report all suspicious activity and security problems.

Physical Access Control{ XE "Physical Access Control" }

Company's office building is monitored 24 hours per day 7 days per week by a security alarm system. During non-business hours, magnetic access cards control physical access to the Company. Each authorized employee is provided with his or her own unique, access card, which can be tracked by the Company. During business hours, access to the office is restricted to the reception area, which is manned by a receptionist.

No non-employee should have unfettered access to the Company's facility. Your guests should be greeted by You in the reception area and escorted to and from any meeting place within the Company. Family members and other non-business guests are also subject to this requirement. Some guests may be issued temporary magnetic access cards for the duration of their visit; however, guest cards must be returned at the end of the guest's presence at Company.

You should enter the Server Room only when You have been authorized to do so by (Network Administrator) or your manager. Access to our Server room is strictly controlled by key locks.

If You handle PHI or IIHI You must have a screen saver that automatically activates after a maximum of 15 minutes with no activity. The screen saver must be set to require a password to reactivate the computer if the workstation is in an open or public area, a cubicle or area that is otherwise generally available to passing traffic.

Company reserves the right to monitor employee use of the computer system at all times.

(Network Administrator) must periodically review user privileges and remove or inactivate accounts when access is no longer required. Managers must inform (Network Administrator) immediately upon the termination of any employee.

(Network Administrator) must implement inactivity time-outs, where technically feasible, for terminals and workstations that access *confidential* information. Managers must work with (Network Administrator) to specify time-out intervals based on business needs and amount of risk and exposure.

Generic access to information stored in databases is allowed only for non-interactive tasks. A non-interactive task is one that is scheduled to run automatically or one that is triggered by a series of events. You do not directly initiate the task, nor are You the direct recipient of the information.

Remote Access/Users{ XE "Remote Access/Users" }

Remote access to Company's computers will be granted to You if You have a demonstrable business need for such access. Permission to access Company's computers remotely is granted by and reviewed periodically by your manager. Company reserves the right to conduct audits to ensure that the requirements for remote access are consistently observed.

Before approval for working at home or telecommuting is granted, Company reserves the right to review the security of the proposed working environment. If You work with sensitive information, a shredder must be available. Similarly, if sensitive information will be stored in paper form, suitable protection from discovery by unauthorized persons must be available or provided by COMPANY. You must also make arrangements to have your files backed-up over the network, or utilize appropriate remote systems to perform your own back-ups.

Remote access to COMPANY computers and networks requires that all Users be definitively authenticated with fixed passwords or other identification systems approved by (Network Administrator). Outbound connection to third party networks including the Internet is permissible through office desktop modems or other types of modems but does not obviate the need to comply with other security precautions related to file downloads and transfers.

Remote users (using VPN) do not get access to the entire network. While You will have access, You will not be able to view the entire network. You will have to know where you want to go on the network if you want access it.
Should You need expanded access to the network when You are remotely accessing the network, You will need to speak with your manager, who will send an e-mail to Network Administrator authorizing same.

Use of the Internet{ XE "Use of the Internet" }

Internet access (beyond electronic mail) will be provided to all employees solely for use to support their work at the Company. Use of the Internet via the network for personal business is not permitted.

Since many staff members will connect to production applications over the Internet, it is important that use be appropriate to Company's business. If You need additional access to Internet facilities, a request should be directed to your manager, who in turn will contact the Network Administrator.

All access and communication to or from the Internet must occur through an actively managed Internet firewall service.

Access via Internet to the internal network must be approved by (Network Administrator). External organizations must have contractual agreements with the Company that address information security, confidentiality and nondisclosure. Access methods must employ strong authentication and encryption. Access must be limited to the minimum systems and services required, and activity must be logged. Internet access by non-entity persons via network services is not allowed. A non-networked system with dialup service to commercial Internet service providers is the preferred method of providing Internet access to non-entity persons.

Company is not responsible for material viewed or downloaded by users from the Internet.

You should schedule communications-intensive activities such as large file transfers, mass e-mailings and streaming audio or video for off-peak times (that is, before 8:00 A.M. and after 7:00 P.M., Monday through Friday). Because audio, video and picture files require significant storage space, files of this sort may not be downloaded unless they are business-related. All files that are downloaded must be scanned for viruses and other destructive programs.

Violation Reporting & Corrective Action{ XE "Violation Reporting & Corrective Action" }

If You have knowledge of an attempted or suspected compromise, theft, vandalism, or misuse or abuse of this Privacy Policy, any protected health information or information technology resources You must initiate a report to your manager and/or the VP of Operations. Reportable incidents include, but are not limited to, the following:

- Unauthorized use of computer time;
- Unauthorized access to sensitive or restricted data;
- Unauthorized modification/alteration of computer data files or programs;
- Detection of non-Company data or programs on a corporate computer system;
- Forgery of negotiable instruments using a computer;
- Theft of computer equipment;
- Disclosure of computer system password to an unauthorized individual;
- Destruction of computer data files or programs.

Employees must complete as much information as possible in the report and not delay in submitting the report for lack of information. These reports should be submitted as soon as possible.

QUESTIONS?

Speak with your manager or the VP, Operations and Legal