

IMPLEMENTATION OF SECURITY RULE PLAN, POLICY AND PROCEDURES

It is the policy of Challenge Industries, Inc. ("Challenge") to ensure the confidentiality, integrity, and availability of all electronic protected health information that Challenge creates, receives, maintains, or transmits; to protect against any reasonably anticipated threats or hazards to the security or integrity of such information; to protect against any reasonably anticipated uses or disclosures of such information that are not permitted under the HIPAA Security Rule; and to ensure compliance with the HIPAA Security Rule by Challenge's workforce.

The following plan, policy and procedures will be effective April 20, 2005 and continue until amended.

SECURITY MANAGEMENT PROCESS

Risk analysis

Challenge has only a moderate risk to electronically-stored protected health information, and has taken steps to ameliorate that risk even further.

The worst possible scenario is a complete loss of all protected health information stored on Challenge's computer system. Such a scenario could be caused by earthquake, fire, or by airplane hitting the building. Any such event is possible but unlikely. However, Challenge has procedures in place to mitigate the effect of such an event. All protected health information is to be stored on the server, not on individual workstation computers. A complete backup of all data stored on the server, including several prior dates and up through the end of the previous business day, is kept off-premises. In addition, we have a contract with Dell to restore the server within a few hours if there is a mechanical failure.

There is some risk to the integrity of protected health information stored on the server. Challenge has taken steps to ameliorate this risk. We allow access only to authorized employees. Employees who are authorized to access protected health information must receive training in Challenge's privacy and security policies. There is some risk remaining of authorized employees, either unintentionally due to ignorance or negligence, or with intentional malice, erasing required files or erasing data or making inaccurate entries within the files. However, this risk is ameliorated by the existence of backup tapes which can be used to restore accurate data. In addition, hard copies of important documents are kept in a locked file room. Employees use the team approach to provide services, and it is the responsibility of every employee who discovers a suspected file problem to report it immediately.

There is a risk of protected health information being exposed to an unauthorized individual. Challenge has taken steps to ameliorate this risk. We allow access only to authorized employees. Employees who are authorized to access protected health information must receive training in Challenge's privacy and security policies. Security measures include locking screensavers, individual passwords, and locked office doors when the employee is away from the office. Employees are responsible to follow Challenge's policy and procedures to keep unauthorized users from using their workstations and/or passwords to access protected health information. The remaining risk is in the e-mailing of protected health information to an unauthorized party. We put the responsibility on our employees to divulge protected health information only as needed for treatment, payment and operations purposes. Our system has the capability to keep a record of e-mails and we may occasionally do a check to make sure that files are sent out of Challenge only for legitimate uses.

Risk management

Challenge will implement the security measures sufficient to reduce the aforementioned risks and vulnerabilities to a reasonable and appropriate level, as detailed in the following sections.

Sanction policy

All violations of Challenge's protected health information security policy will be subject to disciplinary action. Action may range from verbal warnings to termination and referral for criminal prosecution, depending on the nature and circumstances of the violation. Violations of the policy will be reported to the Privacy Officer, who will document the incident and its outcome and take steps to mitigate its effect. The Privacy Officer and the supervisor of the employee who has committed the violation will discuss the disciplinary action to be taken. (For this purpose, "employee" will include any volunteer or contractor over whom Challenge exercises any control or oversight.) The intent of the employee and the actual harm that is done will be fully considered.

If the violation appears to warrant suspension, demotion or termination, documentation of the violation will be given to Human Resources to make sure that the employee's rights are safeguarded according to law. If the employee holds a professional, supervisory or management position, or if referral to the appropriate law enforcement agency for prosecution is suggested, Senior Management will be consulted prior to the disciplinary action being completed.

The extent of any disciplinary action will take the employee's intent into account. However, negligence will not be excused even if it is unintentional. Every employee given access to protected health information has the responsibility of being familiar with the security policy and of being aware of how irresponsible use of the computer system may jeopardize security.

Information system activity review

Challenge's server tracks log-ins. (At the time when this policy first takes effect, the system is set to lock the workstation after five unsuccessful attempts to log in.) The following information is logged about every file stored on the server: who created the file; who last accessed the file; who last modified the file; and who erased the file. This log will be periodically reviewed for anomalies by the Manager of Information Technology. If a problem is reported concerning any file, this information will be available to help reconstruct the activity that compromised its integrity.

ASSIGNED SECURITY RESPONSIBILITY

The person responsible for administering Challenge's Security Policy will be the Privacy Officer. The Manager of Information Technology will be responsible for technical analysis and enforcing the proper use of Challenge's computer system, including the Network Policy.

WORKFORCE SECURITY AND INFORMATION ACCESS MANAGEMENT

Authorization and/or supervision and Workforce clearance procedure

Employees will have access to protected health information in accordance with their need-to-know as defined in the Privacy Rule. This means that some employees may have "read-only" access: this will be determined by someone of Manager or higher level authority. Employees in the Services Department who use the information to provide direct services ("Treatment" under the Privacy Rule) or supervision of direct services will have access to full information regarding the people they serve without restriction. Those employees performing Payment or Operations functions will have access to the minimum information necessary to perform their jobs. Employees without need to know will have no access to electronically-stored protected health information. Questions about a particular employee's need to know will be resolved by the Privacy Officer, who will inform the employee's Manager and the Manager of Information Technology.

Electronically-stored protected health information that needs to be shared outside of Challenge as part of service to a consumer may be electronically transmitted to another service provider participating in treatment (Example: a document sent as an attachment), but only those files actually required to perform the service may be transmitted. The employee must verify the e-mail address before transmitting files.

The information may be transmitted for payment or operations purposes with the same restriction: additional information not needed for the completion of the task may not be transmitted. Each employee is responsible to ensure that only information allowed under the privacy policy (required for treatment, payment or

operations) is transmitted, and that the receiver is the person intended. Additionally, before electronically-stored protected health information may be transmitted for payment or operations purposes to an outside entity, Challenge will implement a Business Associate Agreement with that entity.

Each employee will have his/her own log-in and password, and will have access on the system only to information authorized for that job. Periodically, the system will prompt each user to change the user's password. The Manager of Information Technology will act as administrator of the system, and will make sure that every employee has only required access. Granting of access that varies from that normally expected to be given to the employee may only be authorized by a Manager or person of higher authority, and only when the employee's work requirements justify it. (Example: Corporate Compliance is an operations function, not a treatment function. However, this position requires greater access than other operations functions in order to perform the job.)

It is contrary to Challenge policy for employees to share log-ins and passwords.

Supervisors will have the responsibility to oversee their employees and to make sure that they do not attempt to circumvent the controls on access to protected health information. Any violation, or attempted violation, must be reported to the Privacy Officer and the appropriate disciplinary action must be taken.

Termination procedures

Human Resources shall notify the Manager of Information Technology whenever an employee is terminated or re-assigned to a position that does not require access to protected health information. The employee's manager shall notify the Manager of Information Technology whenever an employee's responsibilities within the department will require a lesser degree of access.

SECURITY AWARENESS AND TRAINING

All new Challenge employees are required to undertake privacy training before they access protected health information. In compliance with the Security Rule, this will include training specifically on security. Employees who started work prior to April 20, 2005 and who have access to protected health information will be given mandatory makeup training on security. This training will include an overview of the Security Rule, procedures to restrict access to electronically-stored protected health information, how to choose and protect passwords, and employees' responsibility to support this policy and to report violations.

Security reminders

Training on Challenge's security policy and procedures is mandatory for all employees who will have access to electronically-stored protected health information. New employees are required to receive training in the privacy policy and security policy before they are allowed access to protected health information. Update training will be given at least once each calendar year.

Protection from malicious software

Bringing removable media into Challenge presents a great risk of introducing viruses to our system. Because of this, floppy disk drives will be disabled on all workstations except when the user has a demonstrated need to use them, and a demonstrated ability and willingness to follow procedures to protect the system in using removable media. The Manager of Information Technology will make the determination whether to allow a user to have a floppy disk drive. Whenever removable media is brought into Challenge which has been used on any computer outside of our system, it must be scanned before it may be inserted into a Challenge machine. Challenge's workstations do this automatically.

Challenge has installed software which will scan e-mails, attachments, and any software proposed for installation for viruses, worms, spyware and other malicious software. Employees are to confer with the Manager of Information Technology or his designated staff backup if in doubt about any e-mail or attachments. No software may be installed on a Challenge computer without the approval of the Manager of Information Technology.

Log-in monitoring

Only users who have been given access by the Manager of Information Technology are able to log in to the system. Challenge's server tracks log-ins. (At the time when this policy first takes effect, the system is set to lock the workstation after five unsuccessful attempts to log in.)

Password management

Each employee will have his/her own log-in and password, and will have access on the system only to information authorized for that job. The Manager of Information Technology will act as administrator of the system, and will make sure that every employee has only required access. Granting of access that varies from that normally expected to be given to the employee may only be authorized by a Manager or person of higher authority, and only when the employee's work requirements justify it.

It is contrary to Challenge policy for employees to share log-ins and passwords.

SECURITY INCIDENT PROCEDURES

Response and reporting

All violations of Challenge's security policy must be documented by the Privacy Officer. Violations include: allowing any individual (including another employee) to have access to protected health information to which the individual is not authorized; sharing log-ins and passwords; attempting to circumvent any computer system controls restricting access; electronically transmitting any protected health information not required for treatment, payment or operations; erasing protected health information stored on Challenge's computer while it is still required for treatment, payment or operations, or failing to take reasonable steps to safeguard its integrity; or any other act or failure to act which either improperly divulges electronically-stored protected health information or endangers its integrity.

CONTINGENCY PLAN

Data Backup plan

All protected health information stored electronically at Challenge shall be stored on the server, not on individual computers. The server has redundant mirrored drives, so that if one fails the other continues to store all recorded information. In addition, the server automatically performs a tape backup of the entire system daily. The Manager of Information Technology or staff designated by him shall take the backup tape from the server daily, shall take it with him when leaving the building and keep it stored in a safe place away from Challenge until the following day's backup tape is ready. Backup tapes are kept for each working day of the past week, the last day of each of the three weeks preceding the current week, and the last day of each of the three months preceding those weeks.

Disaster recovery plan

If one of the mirrored drives becomes damaged, the second drive will continue to store the information until the first one is replaced. In the event the server is irreparably damaged or destroyed in a disaster, the backup tape will be used to replace protected health information.

Emergency mode operation plan

The risk of a disaster destroying the server is small but it does exist. There are two classifications of events which can destroy the server: a localized event in which only the server is destroyed or severely damaged, or an event that destroys or severely damages the entire building.

Challenge does not maintain protected health information which is vital to access within a week or two. (Vital information that may be needed to protect an individual's life or health is a partial duplicate of health information kept by the individual's residence and/or guardian. Protected health information kept exclusively by Challenge is for the purpose of helping individuals to become employable, get and keep a job, etc., and is historical in nature.) If the server is

destroyed or damaged in a localized event, it can be replaced and the protected health information restored within several days. Staff will be able to maintain written records of day-to-day activities until the new server is operating and information is restored.

If there is an event that destroys or severely damages the building, such as a fire, the activities of Challenge will be disrupted for a few weeks. As services to consumers gradually resume, staff will be able to maintain written records of day-to-day activities until a new server can be installed and information restored.

Testing and revision procedures

The Manager of Information Technology keeps a log of requests to restore inadvertently erased files or files with incorrect data. This practice of restoring these files serves as a continuing test of our procedures.

As technology advances or as recognized risks change over time, Challenge will install software upgrades to keep pace with the environment.

Applications and data criticality analysis

Challenge has procedures to restore all needed files.

All protected health information stored electronically at Challenge shall be stored on the server, not on individual computers. The server has redundant mirrored drives, so that if one fails the other continues to store all recorded information. In addition, the server automatically performs a tape backup of the entire system daily. The Manager of Information Technology or staff designated by him shall take the backup tape from the server daily, shall take it with him when leaving the building and keep it stored in a safe place away from Challenge until the following day's backup tape is ready.

Program files are installed on individual workstation computers. Backups of the original installation disks are kept off-site.

EVALUATION

After this policy has been in effect for six months, the Privacy Officer shall perform an initial evaluation of the security policy. Questions to be answered by the evaluation include: whether employees understand the policy and the Security Rule; whether employees are complying with the policy; whether compliance is practicable with the policy as written; and whether there have been any changes to Challenge's operating environment that may necessitate changes to the policy or to procedures to abide by it. Any necessary changes shall be made and implemented.

After the initial evaluation, subsequent evaluations shall be made by the Privacy Officer no less often than every other year to inquire whether there have been any changes to Challenge's operating environment that may necessitate changes to the policy or to procedures to abide by it.

Each evaluation shall be documented and kept with the policy.

BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS

At the time of the initial effective date of this policy, Challenge has no business partners with whom it electronically shares protected health information. Before Challenge begins to electronically share protected health information with any business partner, it will put a Business Associate Agreement into place.

FACILITY ACCESS CONTROLS

All protected health information stored electronically at Challenge shall be stored on the server, not on individual computers. The server is physically protected from intruders by its location in the office of the Manager of Information Technology. This office is located immediately behind the front office, which is attended continually during normal business hours. Before and after normal business hours the door to the building is locked. In addition, the office of the Manager of Information Technology is locked when he is not there.

The server and individual workstation computers, as needed, are protected from power surges and blackouts by individual battery backups. All computers performing critical functions are protected.

A log-in ID and password is required to gain access to the system. Each employee will have his/her own log-in and password, and will have access on the system only to information authorized for that job. The Manager of Information Technology will act as administrator of the system, and will make sure that every employee has only required access, as directed by the Privacy Officer of the employee's Manager or person of higher level authority.

Contingency operations

Challenge does not maintain protected health information which is vital to access within a week or two. (Vital information needed to protect an individual's life or health is a partial duplicate of health information kept by the individual's residence and/or guardian. Protected health information kept exclusively by Challenge is for the purpose of helping individuals to become employable, get and keep a job, etc., and is historical in nature.) If the server is destroyed or damaged in a localized event, it can be replaced and the protected health information restored within several days. Staff will be able to maintain written

records of day-to-day activities until the new server is operating and information is restored.

If there is an event that destroys or severely damages the building, such as a fire, the activities of Challenge will be disrupted for a few weeks. By the time other activities can resume, a new server can be installed and records restored. As services to consumers gradually resume, staff will be able to maintain written records of day-to-day activities until the new server is installed and information restored.

Facility security plan

The building is locked except during business hours. In addition, there is an alarm system. Only employees with a demonstrated need and adequate level of authority are allowed to carry keys to the building and to know the code to disarm the alarm system. Decisions about whether to provide keys and the disarm code to an employee are made by Senior Management (President, Vice President or Directors). During business hours, when the front door is unlocked, the front reception desk is staffed at all times. Access to the building is to be made exclusively through the front door.

Access control and validation procedures

A log-in ID and password is required to gain access to the system. Each employee will have his/her own log-in and password, and will have access on the system only to information authorized for that job. The Manager of Information Technology will act as administrator of the system, and will make sure that every employee has only required access, as directed by the Privacy Officer of the employee's Manager or person of higher level authority.

It is contrary to Challenge policy for employees to share log-ins and passwords.

Individual workstation computers have locking screensavers: the user's password must be used to regain access. Any user leaving the office for an extended period must log off the system.

Supervisors will have the responsibility to oversee their employees and to make sure that they do not attempt to circumvent the controls on access to Protected Health Information. Any violation, or attempted violation, must be reported to the Privacy Officer and the appropriate disciplinary action must be taken.

Maintenance records

The Maintenance Manager will keep records of security-related repairs and modifications, as well as incidents requiring repairs or modifications.

WORKSTATION USE AND WORKSTATION SECURITY

A log-in ID and password is required to gain access to the system. Each employee will have his/her own log-in and password, and will have access on the system only to information authorized for that job. The Manager of Information Technology will act as administrator of the system, and will make sure that every employee has only required access, as directed by the Privacy Officer of the employee's Manager or person of higher level authority.

Challenge's computer system will allow any user who logs in to have access only to files and programs to which the user has been authorized.

DEVICE AND MEDIA CONTROLS

Challenge has laptop computers which may be taken from the building for use by employees at home. All files of protected health information are encrypted and are inaccessible to anyone other than users authorized to have access to the file. These laptops do not have floppy disk drives.

When a laptop is brought back in to Challenge after a file is updated at home, the laptop is connected to the server through a network connection. The operating system will prompt the user whether to update the file on the server to include the changes that were made at home.

Bringing removable media into Challenge presents a great risk of introducing viruses to our system. Because of this, floppy disk drives will be disabled on all workstations except when the user has a demonstrated need to use them, and a demonstrated ability and willingness to follow procedures to protect the system in using removable media. The Manager of Information Technology will make the determination whether to allow a user to have a floppy disk drive. Whenever removable media is brought into Challenge which has been used on any computer outside of our system, it must be scanned before it may be inserted into a Challenge machine. Challenge's workstations do this automatically.

Challenge has installed software which will scan e-mails, attachments, and any software proposed for installation for viruses, worms, spyware and other malicious software. Employees are to confer with the Manager of Information Technology or his designated staff backup if in doubt about any e-mail or attachments. No software may be installed on a Challenge computer without the approval of the Manager of Information Technology.

Only users authorized to have access to files may e-mail copies of those files as an attachment.

Disposal

As of the effective date of this policy, Challenge has no practice of copying protected health information onto floppy disks or other removable media either for use by employees at home or for sharing with other entities for treatment, payment or operations purposes. This practice will not be initiated without the express approval of the Manager of Information Technology. Employees may not copy protected health information onto any removable media.

All data files for business use at Challenge are to be stored on the server. No employee may copy protected health information onto an individual computer, except that files may be copied onto a laptop for work at home. No employee is allowed to copy files from a Challenge laptop onto any removable media.

Before any individual computers are disposed of, the computers will be scanned under the direction of the Manager of Information Technology and all data files will be removed. Following government standard DOD 5200.28-STD, random 0s and 1s will be written over the entire hard disk at least four times.

Media re-use

Before any media that may have contained protected health information is re-used within Challenge or transferred to the control of any entity outside Challenge, it must be re-formatted under the supervision of the Manager of Information Technology. Following government standard DOD 5200.28-STD, random 0s and 1s will be written over the entire hard disk at least four times.

Accountability

Bringing removable media into Challenge presents a great risk of introducing viruses to our system. Because of this, floppy disk drives will be disabled on all workstations except when the user has a demonstrated need to use them, and a demonstrated ability and willingness to follow procedures to protect the system in using removable media. The Manager of Information Technology will make the determination whether to allow a user to have a floppy disk drive. Whenever removable media is brought into Challenge which has been used on any computer outside of our system, it must be scanned before it may be inserted into a Challenge machine. Challenge's workstations do this automatically.

The Manager of Information Technology will keep a record of computers assigned to staff and their user names as they log in. The Manager of Information Technology will also keep track of the use of laptop computers by employees.

Data backup and storage

All protected health information stored electronically at Challenge shall be stored on the server, not on individual computers. The server has redundant mirrored drives, so that if one fails the other continues to store all recorded information. In

addition, the server automatically performs a tape backup of the entire system daily. The Manager of Information Technology or staff designated by him shall take the backup tape from the server daily, shall take it with him when leaving the building and keep it stored in a safe place away from Challenge until the following day's backup tape is ready.

ACCESS CONTROL

Unique user identification

A log-in ID and password is required to gain access to the system. Each employee will have his/her own log-in and password, and will have access on the system only to information authorized for that job. The Manager of Information Technology will act as administrator of the system, and will make sure that every employee has only required access.

It is contrary to Challenge policy for employees to share log-ins and passwords.

Supervisors will have the responsibility to oversee their employees and to make sure that they do not attempt to circumvent the controls on access to Protected Health Information. Any violation, or attempted violation, must be reported to the Privacy Officer and the appropriate disciplinary action must be taken.

Emergency access procedure

The risk of a disaster destroying the server is small but it does exist. There are two classifications of events which can destroy the server: a localized event in which only the server is destroyed or severely damaged, or an event that destroys or severely damages the entire building.

Challenge does not maintain protected health information which is vital to access within a week or two. (Vital information needed to protect an individual's life or health is a partial duplicate of health information kept by the individual's residence and/or guardian. Protected health information kept exclusively by Challenge is for the purpose of helping individuals to become employable, get and keep a job, etc., and is historical in nature.) If the server is destroyed or damaged in a localized event, it can be replaced and the protected health information restored within several days. Staff will be able to maintain written records of day-to-day activities until the new server is operating and information is restored.

If there is an event that destroys or severely damages the building, such as a fire, the activities of Challenge will be disrupted for a few weeks. By the time other activities can resume, a new server can be installed and records restored. As services to consumers gradually resume, staff will be able to maintain written records of day-to-day activities until the new server is installed and information restored.

Automatic logoff

Every employee is expected to use screensavers on their workstations. The length of time before the screensaver appears on the monitor is a function of the risk of an unauthorized party viewing the monitor: the more risk of unauthorized viewing, the sooner the screensaver will appear. Screensavers may only be removed from the screen by logging in with an authorized user name and password. By pressing Alt-Ctrl-Del, the workstation may be locked until the user returns: staff will be expected to lock their screen when leaving the workstation if there is risk of unauthorized viewing.

Encryption and decryption

The files on Challenge's laptop computers are encrypted and accessible only to authorized users. The file, when it is copied from the server on to the laptop, will carry a tag of users authorized to access it.

Protected health information stored on the server can be accessed only by authorized users.

All data files for business use at Challenge are to be stored on the server. No employee may copy protected health information onto an individual computer, except that files may be copied onto a laptop for work at home. No employee is allowed to copy files from a Challenge laptop onto any removable media.

AUDIT CONTROLS

Only users who have been given access by the Manager of Information Technology are able to log in to the system. Challenge's server tracks log-ins. (At the time when this policy first takes effect, the system is set to lock the workstation after twenty unsuccessful attempts to log in.)

The following information is logged about every file stored on the server: who created the file; who last accessed the file; who last modified the file; and who erased the file. If a problem is reported concerning any file, this information will be available to help reconstruct the activity that compromised its integrity.

The Manager of Information Technology will keep a record of computers assigned to staff and their user names. The Manager of Information Technology will also keep track of the use of laptop computers by employees.

The Manager of Information Technology keeps a log of requests to restore inadvertently erased files or files with incorrect data. This practice of restoring these files serves as a continuing test of our procedures.

As technology advances or as recognized risks change over time, Challenge will install software upgrades to keep pace with the environment.

INTEGRITY OF PROTECTED HEALTH INFORMATION

Mechanism to authenticate electronic protected health information

The Challenge Services Department uses a team approach. Staff who provide services to consumers share work and information with each other because this approach provides better services to the people we serve. In addition, the Services Department regularly reviews files to make sure that they are accurate and complete as part of a Corporate Compliance effort. Beyond this, the Corporate Compliance Officer will do a further periodic review of consumer files. If any of these employees suspect that a necessary file has been erased or that correct information has been deleted or incorrect information added to an existing file, the employee has the responsibility to report the file to the Manager of Information Technology or to the appropriate Services Department Manager.

All protected health information stored electronically at Challenge shall be stored on the server, not on individual computers. The server has redundant mirrored drives, so that if one fails the other continues to store all recorded information. In addition, the server automatically performs a tape backup of the entire system daily. The Manager of Information Technology or staff designated by him shall take the backup tape from the server daily, shall take it with him when leaving the building and keep it stored in a safe place away from Challenge until the following day's backup tape is ready. Backup tapes are kept for each working day of the past week, the last day of each of the three weeks preceding the current week, and the last day of each of the three months preceding those weeks.

If any required file has been erased or if an existing file is missing correct information or contains incorrect information, the employee discovering the error will work with the Manager of Information Technology to restore the file as needed, or make corrections based upon notes, personal knowledge and hard copies of the file.

The use of an electronic mechanism to validate software is not necessary or reasonable because of Challenge's team approach to services.

PERSON OR ENTITY AUTHENTICATION

A log-in ID and password is required to gain access to the system. Each employee will have his/her own log-in and password, and will have access on the system only to information authorized for that job. The Manager of Information

Technology will act as administrator of the system, and will make sure that every employee has only required access.

Department managers are responsible to alert the Manager of Information Technology that a new employee will need access to the system.

It is contrary to Challenge policy for employees to share log-ins and passwords.

Supervisors will have the responsibility to oversee their employees and to make sure that they do not attempt to circumvent the controls on access to Protected Health Information. Any violation, or attempted violation, must be reported to the Privacy Officer and the appropriate disciplinary action must be taken.

TRANSMISSION SECURITY

Integrity controls

Challenge's computer system has a firewall to prevent unauthorized access from outside.

It is the responsibility of any employee e-mailing a file as an attachment to an outside entity to verify the identity of the receiver before sending the file. Challenge e-mails are sent with a confidentiality statement as part of the signature.

Only users authorized to have access to files may e-mail copies of those files as an attachment.

Encryption

Encryption of files transmitted to other entities is not necessary or reasonable. Employees are expected to minimize the risks of inadvertent exposure of protected health information to unauthorized persons by following procedures to verify the identity of the intended recipient. The nature of Challenge's protected health information is unremarkable and there is very little risk of anyone attempting to intercept transmitted files.

DOCUMENTATION

Time limit

This plan and policy (with any amendments) shall be maintained in written form indefinitely (until Challenge is dissolved, HIPAA is repealed, or equivalent event). Any action, activity or assessment required by the Security Rule to be documented shall be maintained with the plan, policy and procedures for a minimum of six years.

Availability

The complete set of documentation shall be made available to the Privacy Officer, Manager of Information Technology, Maintenance Manager, Human Resources Associate and any other employees responsible for any part of the security plan.

Updates

After this policy has been in effect for six months, the Privacy Officer shall perform an initial evaluation of the security policy. Questions to be answered by the evaluation include: whether employees understand the policy and the Security Rule; whether employees are complying with the policy; whether compliance is practicable with the policy as written; and whether there have been any changes to Challenge's operating environment that may necessitate changes to the policy or to procedures to abide by it. Any necessary changes shall be made and implemented.

After the initial evaluation, subsequent evaluations shall be made by the Privacy Officer no less often than every other year to inquire whether there have been any changes to Challenge's operating environment that may necessitate changes to the policy or to procedures to abide by it.

Each evaluation shall be documented and kept with the policy.