IMPLEMENTATION OF SECURITY RULE
PLAN, POLICY AND PROCEDURES

It is the policy of Challenge to ensure the confidentiality, integrity, and availability of all electronic protected health information that Challenge creates, receives, maintains, or transmits.

SECURITY MANAGEMENT PROCESS

Risk analysis
Challenge has 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. A complete backup of the previous days data stored on the server is kept off-premises.

We allow access only to authorized employees and 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 backups which can be used to restore accurate data. In addition, hard copies of important documents are kept locked in the finance room. It is the responsibility of every employee who discovers a suspected file problem to report it immediately.

Security measures include screensavers, individual passwords, and locked office doors when the employee is away from the office. 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. E-mails can now be sent, fully encrypted using Azure Information Protection.

Every 90 days your e-mail will require a change of password (you will be given a fortnights (2 weeks) notice) – if you do not change your password within this period you will be locked out of the system and will need to ask the Manager of Information Services to reset it. Choose a password that is memorable but complex. Passwords must have at least one of each: Uppercase, lowercase, number and adding a character makes it even stronger.

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.

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.

ASSIGNED SECURITY RESPONSIBILITY

The Manager of Information Services will be responsible for technical analysis and enforcing the proper use of Challenge's computer system, including the Network Policy.

Electronically stored protected health information that needs to be shared outside of Challenge may be electronically transmitted to another service provider participating in treatment using encrypted e-mail.or via fax or the US Postal Service.

Termination procedures

Human Resources shall notify the Manager of Information Services 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 Services 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 mandatory privacy training before they access protected health information.

Protection from malicious software

Bringing removable media into Challenge presents a great risk of introducing viruses to our system. Because of this, all removable media including USB drives, cell phones and cameras are not allowed to be connected to the network except when the user has a demonstrated need to use them. Whenever removable media is brought into Challenge it must be scanned before it may be used on Challenge's Network.

Challenge has anti-malware software which will scan e-mails, attachments, and any software prior to viewing/installing for viruses, worms, spyware and other malicious software.

Our Checkpoint internet appliance, also blocks malicious threats.

CONTINGENCY PLAN

Data Backup plan
All protected health information is stored on the server, not on individual computers. And is backed up continually to an offsite location.

Emergency mode operation plan
The risk of a disaster destroying the server is small but it does exist.
If the server is destroyed 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.

Testing and revision procedures
The Manager of Information Services 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.

POLICY REVIEW

This policy shall be reviewed and updated on a biannual basis by the Compliance Officer and Manager of Information Services.

Facility security plan
The building is locked except during business hours. In addition, there is computerized key pad for employees to enter the building outside of normal work hours. Only employees with a demonstrated need have the code to the keypad. Decisions about whether to provide the code to operate the key pad are made by the leadership team. During business hours, when the front door is unlocked, the front reception desk is staffed at all times.

Disposal/Re-use

Before any individual computers are disposed of, the computers will be scanned under the direction of the Manager of Information Services and all data files will be removed. The hard drives are then wiped following government standard DOD 5200.28-STD, random 0s and 1s will be written over the entire hard disk.

Logging off
Every employee is expected to use screensavers on their work stations, screensavers may only be removed from the screen by logging in with an authorized user with 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 their areas.

Encryption and decryption
The files on Challenge's laptop computers are encrypted using BitLocker and accessible only to authorized users.

INTEGRITY OF PROTECTED HEALTH INFORMATION

Mechanism to authenticate electronic protected health information
The Challenge Employment and Vocational Supports (EVS) 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 EVS Department regularly reviews files to make sure that they are accurate and complete as part of a Corporate Compliance effort. Beyond this, the QA Associate 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 immediately report the file to the Manager of Information Services or to the appropriate EVS Manager.

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

Challenge uses an EMR (Electronic Medical Record) cloud based system provided by Precision Care and all records are secured and backed up by Precision Care.

Updates
Periodic 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. 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.

Each evaluation shall be documented and kept with the policy.

STANDARDS FOR PHI IN INDIVIDUAL STAFF WORK AREAS

Staff are expected to make a reasonable and conscientious effort to safeguard Protected Health Information in their possession. They should adhere to the following minimum guidelines, but should use their best judgment in exceeding these guidelines when a specific situation requires.

Each staff member should keep a desk drawer available which may be used to slide PHI into. PHI should never be left on a desktop when the staff member leaves their office or area without closing the door or securing files.

Staff should close their office doors any time they leave the office.

Staff may, under their best judgment, allow consumers to sit in their office/area for a period of time unattended. PHI should be placed inside a closed drawer, and the staff member should remain nearby to check on the office periodically. If there is doubt about the consumer's ability to sit for a period of time without looking into drawers, then all PHI should be locked up.

Staff should assist each other by keeping a watchful eye on other offices in their vicinity. They have the authority to investigate any questionable activity in another staff member's office.

At the end of each workday, all PHI must be locked. It may be locked in a desk drawer, in an individual office, or in the finance room.

The finance room must be locked at the end of each day.