



MAILING ADDRESS / DIRECCION DE CORREO

P.O. BOX 8332,
FALLS CHURCH, VA 22041

PHONE: (571) 388-8292
FAX: (703) 997-7122
INFO@CULMORECLINIC.ORG
WWW.CULMORECLINIC.ORG

CULMORE CLINIC SECURITY POLICY

USER LOGON IDS

Individual users shall have unique logon IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier which will be an email with a Culmore Clinic extension.
- Users shall be responsible for the use and misuse of their individual logon ID.
- All user login IDs are audited at least twice yearly and all inactive logon IDs are revoked as soon as the employee or the volunteer leaves the Clinic.
- The logon ID is locked or revoked after a maximum of three (3) unsuccessful logon attempts which then require the password to be reset by the System Administrator.

PASSWORDS

User Account Passwords

User IDs and passwords are required in order to gain access to all Practice Fusion networks and workstations. All passwords are restricted by a clinic-wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

- Password Length – Passwords are required to be a minimum of eight characters.
- Content Requirements - Passwords must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.
- Change Frequency – Passwords must be changed every 90 days. Compromised passwords shall be changed immediately.
- Reuse - The previous 3 passwords cannot be reused.
- Restrictions on Sharing Passwords - Passwords shall not be shared, written down on paper, or stored within a file or database on a workstation and must be kept confidential.
- Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens, and are never printed or included in reports or logs. Passwords are stored in an encrypted format.

USER PRACTICES AND PROCEDURES

Browsing The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The Clinic has access to patient level health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.

Office Practices

- Paper faxes received at the Clinic will be removed from the Fax machine as soon as possible.
- Paper faxes, if it is patient information, will be scanned into the appropriate client record in the EHR.
- E-Fax's containing patient information will be moved from the desktop to the EHR to the appropriate client file and then deleted from the desktop in a timely manner.
- Emails cannot include patient information without encryption because they are not secure.
- Logging into the EHR from your cell phone is prohibited.
- Access to Practice Fusion from a public WiFi site is prohibited.
- Interpreters may not discuss patient information outside of the patient encounter except with the Clinic staff, as needed.
- All paper medical records will be in a locked cabinet outside of clinic hours.



MAILING ADDRESS / DIRECCION DE CORREO

P.O. BOX 8332,
FALLS CHURCH, VA 22041

PHONE: (571) 388-8292
FAX: (703) 997-7122
INFO@CULMORECLINIC.ORG
WWW.CULMORECLINIC.ORG

Software Malfunction Users should inform the System Administrator when Practice Fusion does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or staff, suspects a computer virus infection, the Clinic computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the System Administrator as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

PERSONAL HEALTH INFORMATION

As directed by HIPAA, all personal identifying information is removed from all data that falls within the definition of PHI before it is stored or exchanged. De-identification is defined as the removal of any information that may be used to identify an individual or of relatives, employers, or household members.

PHI includes:

Names
Addresses
Geographic subdivisions smaller than a state
All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)
Telephone numbers
Facsimile numbers
Driver's license numbers
Electronic mail addresses
Social security numbers
Medical record numbers
Health plan beneficiary numbers
Account numbers, certificate/license numbers
Vehicle identifiers and serial numbers
Device identifiers and serial numbers
Web Universal Resource Locators (URLs)
Internet Protocol (IP) address numbers
Biometric identifiers
Full face photographic images and any comparable images

Telecommuting and Practice Fusion

Telecommuting employees/volunteers are required to follow all Clinic corporate, security, confidentiality, or Code of Conduct policies that are applicable to all other employees and volunteers:

- All Clinic staff and volunteers must have written authorization from the Clinic Director to open Practice Fusion anywhere but on the Clinic premises.
- Telecommuting Users will have the access based on the same 'need to know' as they have when in the office.



MAILING ADDRESS / DIRECCION DE CORREO

P.O. BOX 8332,
FALLS CHURCH, VA 22041

PHONE: (571) 388-8292
FAX: (703) 997-7122
INFO@CULMORECLINIC.ORG
WWW.CULMORECLINIC.ORG

- Password Use: The use of a strong password, changed at least every 90 days, is even more critical in the telecommuting environment. Do not share your password or write it down where a family member can see it.
- If personal devices are used to access Practice Fusion, they must have current virus and malware protection.
- Training: Personnel who telecommute must complete the same annual privacy training as all other employees.

USE OF TRANSPORTABLE MEDIA

Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB key devices. Every workstation that has been used by Clinic employees or volunteers is presumed to have sensitive information stored on its hard drive. Therefore procedures must be carefully followed when copying data to or from transportable media to protect sensitive Clinic data.

All users must be aware that sensitive data could potentially be lost or compromised when moved outside of Clinic computers. Transportable media received from an external source could potentially pose a threat to the Clinic computers. **Sensitive data** includes all human resource data, financial data, and personal health information ("PHI") protected by the Health Insurance Portability and Accountability Act ("HIPAA").

Rules governing the use of transportable media include:

- All USB keys used for Clinic business will be owned by the Clinic.
- No Clinic employees or volunteers will use a USB key without authorization from the Clinic Director.
- No **sensitive data** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- The use of a personal USB key is prohibited.
- Users connecting to a device not owned by the Clinic must maintain current virus and malware protection.
- Report any loss of transportable media to the System Administrator.
- When an employee resigns from the Clinic, all transportable media must be returned to the Clinic.

RETENTION / DESTRUCTION OF MEDICAL INFORMATION

Many state and federal laws regulate the retention and destruction of medical information. The Clinic actively conforms to these laws and follows the strictest regulation if/when a conflict occurs.

Record Retention - Documents relating to uses and disclosures, authorization forms, health information, business partner contracts, notices of information Clinic, responses to a patient who wants to amend or correct their information, the patient's statement of disagreement, and a complaint record are maintained for a period of 6 years after the patient is last seen at the Clinic.

CONTINGENCY PLAN

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain ePHI.

The Clinic is committed to maintaining formal practices for responding to an emergency or other occurrence that damages systems containing ePHI. The Clinic shall continually assess potential risks and vulnerabilities to protect health information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule. The Clinic Director shall implement a backup plan to create and maintain a process for accessing Practice Fusion in the event of an emergency or an alternative back up plan for continuing to operate the Clinic.

The System Administrator shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of:



MAILING ADDRESS / DIRECCION DE CORREO

P.O. BOX 8332,
FALLS CHURCH, VA 22041

PHONE: (571) 388-8292
FAX: (703) 997-7122
INFO@CULMORECLINIC.ORG
WWW.CULMORECLINIC.ORG

1. Restoring or recovering any loss of ePHI and/or systems necessary to make ePHI available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and
2. Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained on-site and at the off-site locations at which backups are stored or other secure off-site location.

VIOLATIONS

- When appropriate, progressive disciplinary action steps shall be followed allowing the employee/volunteer to correct the behavior which caused the disciplinary action.
- Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with the Clinic.

References

U.S. Department of Health and Human Services
Health Information Privacy. Retrieved April 24, 2009, from
<http://www.hhs.gov/ocr/privacy/index.html>

Acknowledgment

I have signed a copy of the EMPLOYEE/VOLUNTEER CONFIDENTIALITY AGREEMENT for the Culmore Clinic which includes a statement that I have received a copy of this Security Policy document.



MAILING ADDRESS / DIRECCION DE CORREO

P.O. BOX 8332,
FALLS CHURCH, VA 22041

PHONE: (571) 388-8292
FAX: (703) 997-7122
INFO@CULMORECLINIC.ORG
WWW.CULMORECLINIC.ORG

CULMORE CLINIC VOLUNTEER AGREEMENT

Culmore Clinic strives to provide the highest quality care possible to its clients. The Clinic relies on a carefully selected and dedicated staff of volunteers to make this happen.

Volunteers are expected to:

1. Provide a list of days that they can volunteer (6 week increments).
2. Students are requested to alert the clinical director (no later than 24 hours, by email or phone), when they need to cancel their shift.
3. All volunteers must sign-in on the sheet located in the office (taped on refrigerator) to track hours worked.

Although the Clinic tries to maintain a relaxed approach to scheduling, our clients need us to be present. Every person is important to the Culmore Clinic's efficiency. Signing below is your agreement to take your volunteer position responsibly.

Print Name: _____ Date: _____

Signature: _____



MAILING ADDRESS / DIRECCION DE CORREO

P.O. BOX 8332,
FALLS CHURCH, VA 22041

PHONE: (571) 388-8292
FAX: (703) 997-7122
INFO@CULMORECLINIC.ORG
WWW.CULMORECLINIC.ORG

Volunteer & Staff Information

Current Date: _____

Name: _____ As it appears on any license application. Nickname: _____

Mailing Address: _____

Best to contact by: email____cell____

Home phone_____Work phone_____Cell:_____Other: _____

Email: _____ Birthday (Month/Day):_____

Languages Spoken: _____

For Volunteers: Please note which Volunteer Position interests you:

Preferred Shift: _____10:00 am - 2:00 pm; _____3:00 pm – 7:00 pm

___ **Interpreter** Language(s):_____ Certified?_____

___ **Nurse:** RN, BSN, ARNP / License Number:_____ Eff Date:_____ Specialty:_____

___ **Medical Doctor:** License Number:_____ State:_____ Specialty:_____

___ **Set UP Ministry;** or Other Position:_____



MAILING ADDRESS / DIRECCION DE CORREO

P.O. BOX 8332,
FALLS CHURCH, VA 22041

PHONE: (571) 388-8292
FAX: (703) 997-7122
INFO@CULMORECLINIC.ORG
WWW.CULMORECLINIC.ORG

Thank you for your interest in Culmore Clinic and its mission!