

## **ELECTRONIC DATA SECURITY**

**POLICY:** ADEC will, to the best of its knowledge and awareness protect Electronic Protected Health Information from unauthorized access, modification disclosure, and destruction.

Responsible: Informational Technology Services Manager  
Latest Rev: 4/12/2023  
Approved:

**PURPOSE:**

To protect all Protected Health Information (PHI) in the possession of ADEC, and stored on electronic media. ADEC will protect electronic PHI (e-PHI) from unauthorized access, modification, disclosure, and destruction. This Policy outlines specific procedures to protect the PHI.

Violations of this policy may lead to termination of employment.

**PROCEDURE:** Security Requirements.**I. Access to PHI and Security.****A. Computer network.**

Each user will be assigned a unique identifier (user name) and password. Passwords must be changed at least once a year (see II. Passwords). Access to computers, drives, and folders on network computers will be based on Access Level (see IV. Access Control).

**B. Workstation Use and Security for Computers located at an ADEC Facility.**

1. Workstations includes desktop computers, laptop computers and mobile devices. The assignment of a workstation is determined by an assessment of user need conducted by the Information Technology Services Department and recommendations by the appropriate Vice President.
2. Physical Location. The preferred location is for the computer to be located in an office with a locked door. If the computer is located in a non-secure area, additional security precautions should be taken as outlined in the section C. Additional Workstation Security for Computers and mobile devices located outside ADEC Facilities.
3. Workstations should be located in a manner that inhibits others from incidentally viewing another person's e-PHI on workstations. Additional devices such as screen filters should be considered for workstations located in an area open to the public.
4. Data Storage. All e-PHI data should be stored on the ADEC computer network drives if available. If e-PHI data is stored on a local computer drive (drive C of the computer), additional encryption is required; and the employee is responsible for secure data backups and storage (see III. Media Controls).
5. Inactivity time-outs. All computers and mobile devices that access e-PHI must have inactivity time-outs set to 15 minutes or less, where technically feasible.
6. Passwords. Passwords must be changed at least once a year (see II. Password).
7. Placement and inventory of Workstations and portable devices will be maintained and reviewed by the ADEC Information Technology Services Department. This includes the inventory of all devices that contain e-PHI and where the device resides.

**C. Additional Workstation Security for computers and mobile devices located outside ADEC Facilities.**

1. Approval. The Information Technology Services Manager will review and approve the placement of devices located outside ADEC Facilities.

2. Encryption. If e-PHI data is stored on a workstation or mobile device additional device encryption and access passwords are required. The ADEC Information Technology Services Department will verify encryption and keep an inventory of encrypted devices.
3. Data Backup. The employee is responsible for secure data backups and storage (see III. Media Controls) of all e-PHI stored on the local computer.
4. Laptop computers and mobile devices that contain e-PHI should be transported by employees in a secure manner. Reasonable care should be used and laptops and mobile devices should be secured when left unattended.

D. Computers or portable mobile devices owned by employees

1. ADEC provides the tools staff need to do their work within the agency “network” of hardware and software. However, for staff convenience and efficiency ADEC allows for the use of employee personal devices to connect via a secure connection to the visitor wifi only. Currently this is limited to an employee connecting to the ADEC e-mail to view e-mail, MyMITC for the Web, and ADP Employee Portal.
2. Employees are **not** to download and store Electronic Protected Health Information (e-PHI) on a non ADEC computer or personal portable device.

## II. Passwords.

Passwords are the user’s responsibility and may not be shared, unless expressly authorized by ADEC. Users will be able to select and change their passwords. It is required that passwords be changed annually. Permanent passwords are not permitted. Passwords will be at least eight characters long. In that 8 or more characters, passwords should typically contain at least three of the following: upper case, lower case, symbols and numbers. Use of numeric digits and non-alphanumeric characters in passwords is highly encouraged. Users should not write down passwords, store them on hardcopy or store them locally on workstations and laptop computers.

Passwords include network passwords, Windows passwords, startup passwords, an inactivity time-out password, and file password protection. In addition, Users are responsible to change the passwords to access specific software (example ADP, Blackbaud, Sandata, MyMITC for the Web).

The following passwords can be the same password as long as the password is not shared with other users. It is recommended that users choose a unique password for ADEC sites, and not use the same password as non ADEC sites (example social media password).

### Definition of passwords.

Network password. Used to authenticate the user to the ADEC network, used in conjunction with the user name (last name, first initial). The network system will force the user to change this password at least once a year.

Windows password. This is the password on a Windows computer. This password must be the same as the Network password.

Startup password. This is a power-up password that is part of the BIOS setup of the computer. This keeps the computer from starting until this password is entered.

Inactivity time-outs and password. This password is set with the computer screen saver. This is found with Microsoft Windows 10 on the Settings: Personalization – Lock Screen – Screen Saver Setting, turning on password protect. The Inactivity time-outs should be set to 15 minutes or less.

File password protection. This password is saved as part of the document. This password is needed to open the document. File password protection is an option to give additional security. This is important for files containing e-PHI saved on local computer (drive C), computers located at remote sites.

Application Passwords. Many of the software applications (example ADP, Blackbaud, Sandata, MyMITC for the Web) also require a password. When the user changes the Windows and Network password, the application password will not change automatically, as the user will need to change those passwords within the software. It is recommended the user change application passwords at the same time as changing the Network password.

E-mail password. The Microsoft Office 365 password gives access to the employee's ADEC e-mail. For those require to use a Network password, the e-mail password will be the same. For employees who only have an e-mail account, this password will be changed on the Microsoft Office 365 site.

Multifactor Authentication. ADEC will utilize Multifactor Authentication where technically feasible. This includes Microsoft Office 365 and other remote access systems. Multifactor Authentication will require the ADEC employee to authenticate a second time using a phone or other device to confirm their identity and grant access to use the system. For Office 365 an employee will setup the initial Multifactor Authentication using the phone number of their primary ADEC work location, additional optional Multifactor Authentication can be setup and used with a personal cell phone.

### **III. Media Controls.**

1. Hardcopy of PHI should not be copied indiscriminately or left unattended and open to compromise.
2. PHI in Hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.
3. Data backups that contain PHI must be stored in a secure location, preferably in a locked filing cabinet or safe.

### **IV. Access Controls.**

Access to e-PHI will be set according to the role appropriate for the employee and the user's need to know. The user's need to know will be verified by the Information Technology Services Department before least privileges are granted.

The Information Technology Services Department will determine Access level in consultation with the Supervisor, employee responsible for the application or data security, and the appropriate Vice President.

Each person who is entitled to access information possessed by ADEC will be assigned an Access level based on their position, role, and/or responsibility. The ADEC Information Technology Services Manager will implement policies and procedures to authorize members of ADEC's workforce to access the minimum amount of electronic protected health information necessary to perform their job duties.

The Information Technology Services Department will oversee the access control of ADEC information systems utilizing built-in security settings for access control of the various software systems. When possible, the security settings will be reviewed by two members of the Information Technology Services Department.

Access control includes unique identification of users and utilizing available authentication methods. A user will be required to enter a unique identifier when accessing ADEC information systems.

Employees will have access to their own computer or workstation as needed.

Employees will have access to their network Home account (Drive H:).

Employees will be granted access to shared folders based on the discretion of the Information Technology Services Department in consultation with the manager or owner of the shared folder.

Employees are expected to store and transmit Protected Health Information (PHI) only within the ADEC network. In situations where there is a need to store or transmit PHI information outside the ADEC network, the Information Technology Services Manager will review and approve those procedures.

Access to the Agency Individuals Served Data base will be set according to Access level needed to perform the job. Generally, access to individuals served information will only be granted to staff on a Need to Know basis if they are, have been, or will be involved in that individual's served care.

The Information Technology Services Manager will enact procedures designed to ensure that, when a member of ADEC's workforce is separated from ADEC for any reason whatsoever that person's access to electronic protected health information is foreclosed. The timing for removing security is preferably the end of the employee's final shift.

## **V. Contingency Plan.**

**Data backup plan.** All data and application software on the ADEC network computers will be backed-up at least nightly as outlined in the ADEC Disaster Recovery and Business Continuity Plan; including the rotation of the backup generations. Backup of any data stored on desktop and laptop computers will be the responsibility of the computer user.

**Disaster Recovery Plan.** The ADEC Disaster Recovery and Business Continuity Plan document is the plan of ADEC for response, recovery, resumption, restoration, and return after severe disruption. The ADEC e-mail system is hosted by Microsoft Office 365 with business continuity and data backup responsibilities provided by Microsoft; in the event of a local disruption e-mail will remain available through an internet connection. Other ADEC systems hosted by various vendors with business continuity and data backup responsibilities provided by

the vendors include Blackbaud, ADP, Sandata, ACCUflo eMAR; in the event of a local disruption these systems will remain available through an internet connection

Test of the ADEC Disaster Recovery and Business Continuity Plan. A test will be conducted at least annually and will include a written analysis. The written analysis will include effectiveness, areas needing improvement, actions to address the improvements needed, implementation of those actions, documentation of whether the actions taken accomplished the intended results, necessary education and training of personnel.

## **VI. Event Monitoring and System Activity.**

The Information Technology Services Department will periodically review event logs to identify potential security issues or monitor system and application activities.

This includes network login monitoring and review of activity logs for software applications.

## **VII. Media Disposal and re-use.**

The ADEC Information Technology Department will be responsible for device disposal and re-use.

Workstation storage disks that are no longer needed will be locked up until they are disposed. Disposal can be electronic reformatting of the media according to generally accepted sanitizing practices; or physically disabled or destroyed.

Before workstation storage disks can be re-used, the ADEC Information Technology Services Department will prepare the media. This will be electronic reformatting of the media according to generally accepted sanitizing practices.

## **VIII. Movement of Media containing e-PHI.**

Records will be maintained by the Information Technology Services Department when media containing e-PHI is moved outside an ADEC Facility. This includes an inventory of laptops and portable devices; and movement of e-PHI on other media such as tapes or computer disks.

If off-site maintenance is needed for media containing e-PHI, the e-PHI will be backed up, removed, or security measures taken; before the media is removed from an ADEC facility. ADEC will rely upon the retrievable exact copies created as part of its routine back-up. In the event of loss of electronic protected health information due to a move of equipment, ADEC will restore the lost information from ADEC's regularly performed back-up. In most situations, the ADEC Information Technology Services Department will perform a back-up right before any computer hardware or other equipment containing electronic protected health information is moved off site.

Maintain a record of the movements of hardware and electronic media within ADEC's facility. For movement of hardware and electronic media for Computer Servers that house the ADEC Electronic Protected Health Information, the Information Technology Services Manager will maintain a record of the movements of hardware and electronic media. For computer workstations included desktop and laptop computers, the Information Technology Services Department will maintain an inventory of the location of those devices.