Highlights of PHI/PI Security Requirements

These guidelines are excerpts from ACBHCS's contract with the CA DHCS and applies to all ACBHCS contract providers as well as County clinics. For more detailed requirements, please see attached *Exhibit F: Privacy and Information Security Provisions, Attachment A: Business Associate Data Security Requirements*. Please consult with an IT specialist to make sure your agency is in compliance with HIPAA and HITECH regulations.

Technical Security Controls

- **Workstation/Laptop Encryption.** All workstations and laptops that store PHI or PI either directly or temporarily must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the CA Department Information Security Office.
    - ***Encrypting the documents only is not enough***
    - ***Encryption of documents through Microsoft Word 2007 is NOT enough***
    - ***Encryption of documents and password protection is NOT enough***
    - ***Encryption solution MUST be full disk encryption (FDE)***

- **Minimum Necessary** Only the minimum necessary amount of PHI or PI may be copied, downloaded, or exported in order to do the work at hand.

- **Removable media devices** All electronic files that contain PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128 bit or higher such as AES.

- **Transmission encryption** All data transmissions of PHI or PI outside a secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-mail.

Paper Document Controls

- **Supervision of Data** PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information.

PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airlines.

- ***Alameda County BHCS requires that clinical records be stored in a "double locked" manner (e.g., in a locked filing cabinet located within a locked office).***

- ***Alameda County BHCS requires that if records must be transported, maintain the "double locked" and safeguarding requirement (e.g., transported in a locked box in a locked vehicle trunk and not left in an unattended vehicle). Laptop computers must have full disk encryption, be password protected and transported in a locked vehicle trunk.***

What to do in Case of a Suspected or Actual Breach or Security Incident

Breach: *The access or acquisition of any unsecured PHI or PI in electronic media or in any other media by an unauthorized person.*

Security Incident: *The attempted or successful unauthorized access, use, disclosure, modification or destruction of PHI/PI; or interference with system operations in an information system that processes, maintains or stores PHI.*

Immediately upon discovery of a suspected or actual breach or security incident, County providers and contracted providers **must**:

- Call ACBHCS Quality Assurance Office at (510) 567-8105 to report the incident (leave a message if after business hours, weekend, or holiday).
- E-mail or fax a Privacy Incident Report (PIR), with as much information as is known at the time **to ACBHCS at** BreachNotification@acgov.org or fax to (510) 639-1346.
  Link to CA DHCS PIR form at: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Documents/Privacy-Incident-Report-(PIR)-2014.pdf
- ACBHCS will in turn, notify the CA DHCS of the incident & submit the required Privacy Incident Report to the CA DHCS.

In the next 2 working days:

- Continue to investigate the incident to obtain as much information as possible. The information you gather will assist in determining if a breach did occur.
- By the end of the second working day, send an updated PIR to ACBHCS Quality Assurance.
- ACBHCS staff will file the required updated Privacy Incident Report to the DHCS that is due within 72 hours of the discovery.

During the next 7 working days:

- Continue to investigate the incident in your agency/clinic.
- If needed, begin to formulate a Mitigation Strategy and Corrective Action Plan
- County staff will also investigate and may ask you questions regarding facts about the incident, security measures that were in place at the time, current relevant policies and procedures, police reports that were filed, any other reporting done, details of your agency's Mitigation Strategy and Corrective Action Plan, etc.
- County staff will file a complete PIR with the DHCS within ten (10) working days of the discovery of the incident or later if more time is needed.

DO NOT:

- Do not contact CA DHCS directly regarding the privacy incident as it is ACBHCS's responsibility to notify them.
- Do not send out notification letters to affected individuals until you have submitted a sample notification letter to ACBHCS and the letter has been reviewed and approved by DHCS.

ACBHCS Contact for Privacy Incidents:

Attn: QA Associate Administrator
Phone: (510) 567-8105
FAX: (510) 639-1346
E-mail: BreachNotification@acgov.org

Please note that guidelines in ACBHCS HIPAA Breach Reporting Policy dated 7/25/13 (and posted online) are incorrect and are currently being revised. For questions or concerns, please contact ACBHCS QA as listed above.

EXHIBIT F
Privacy and Information Security Provisions

Attachment A
Business Associate Data Security Requirements

1. Personnel Controls

A. **Employee Training**. All workforce members who assist in the performance of functions or activities on behalf of the Department, or access or disclose Department PHI or PI must complete information privacy and security training, at least annually, at Contractor's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following termination of this Agreement.

B. **Employee Discipline**. Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

C. **Confidentiality Statement**. All persons that will be working with Department PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to Department PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for Department inspection for a period of six (6) years following termination of this Agreement.

D. **Background Check**. Before a member of the workforce may access Department PHI or PI, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years.

2. Technical Security Controls

A. **Workstation/Laptop encryption**. All workstations and laptops that store Department PHI or PI either directly or temporarily must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the Department Information Security Office.

B. **Server Security**. Servers containing unencrypted Department PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

EXHIBIT F
Privacy and Information Security Provisions

C. **Minimum Necessary**. Only the minimum necessary amount of Department PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

D. **Removable media devices**. All electronic files that contain Department PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

E. **Antivirus software**. All workstations, laptops and other systems that process and/or store Department PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

F. **Patch Management**. All workstations, laptops and other systems that process and/or store Department PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release. Applications and systems that cannot be patched within this time frame due to significant operational reasons must have compensatory controls implemented to minimize risk until the patches can be installed. Applications and systems that cannot be patched must have compensatory controls implemented to minimize risk, where possible.

G. **User IDs and Password Controls**. All users must be issued a unique user name for accessing Department PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed at least every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

1) Upper case letters (A-Z)
2) Lower case letters (a-z)
3) Arabic numerals (0-9)
4) Non-alphanumeric characters (punctuation symbols)

H. **Data Destruction**. When no longer needed, all Department PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the Department Information Security Office.

EXHIBIT F
Privacy and Information Security Provisions

I. **System Timeout**. The system providing access to Department PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

J. **Warning Banners**. All systems providing access to Department PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

K. **System Logging**. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for Department PHI or PI, or which alters Department PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If Department PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

L. **Access Controls**. The system providing access to Department PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

M. **Transmission encryption**. All data transmissions of Department PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing Department PHI can be encrypted. This requirement pertains to any type of Department PHI or PI in motion such as website access, file transfer, and E-Mail.

N. **Intrusion Detection**. All systems involved in accessing, holding, transporting, and protecting Department PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. **Audit Controls**

A. **System Security Review**. Contractor must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing Department PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

B. **Log Reviews**. All systems processing and/or storing Department PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

C. **Change Control**. All systems processing and/or storing Department PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

EXHIBIT F
Privacy and Information Security Provisions

4. Business Continuity / Disaster Recovery Controls

A. **Emergency Mode Operation Plan.** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of Department PHI or PI held in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

B. **Data Backup Plan.** Contractor must have established documented procedures to backup Department PHI to maintain retrievable exact copies of Department PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore Department PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of Department data.

5. Paper Document Controls

A. **Supervision of Data.** Department PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Department PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B. **Escorting Visitors.** Visitors to areas where Department PHI or PI is contained shall be escorted and Department PHI or PI shall be kept out of sight while visitors are in the area.

C. **Confidential Destruction.** Department PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

D. **Removal of Data.** Only the minimum necessary Department PHI or PI may be removed from the premises of the Contractor except with express written permission of the Department. Department PHI or PI shall not be considered "removed from the premises" if it is only being transported from one of Contractor's locations to another of Contractors locations.

E. **Faxing.** Faxes containing Department PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

F. **Mailing.** Mailings containing Department PHI or PI shall be sealed and secured from damage or inappropriate viewing of such PHI or PI to the extent possible.

EXHIBIT F
Privacy and Information Security Provisions

Mailings which include 500 or more individually identifiable records of Department PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of the Department to use another method is obtained.

Buyer's Guide to Full Disk Encryption

Don't let a lost or stolen laptop put your business at risk. Here's how to prevent a data breach by encrypting your organization's hard drives.

By **Paul Rubens** | Posted May 09, 2012

When a corporate laptop goes missing, do you worry about the risk of a data breach? There is good reason for concern: According to recent research by Symantec, 34 percent of data breaches are the result of lost or stolen devices such as laptops.

The good news is that this is a preventable issue. A Full Disk Encryption (FDE) solution can ensure that sensitive information isn't exposed in the event that one of your organization's laptops is lost or stolen.

How It Works

As the name suggests, FDE solutions work by encrypting a system's entire hard drive – including the operating system and all applications and data stored on it. When the system is started, the user is prompted for the encryption key, which enables the system to boot and run normally. As information is read from the disk, it is decrypted on the fly and stored in memory – and any information written to the disk is also encrypted on the fly. Without the encryption key, the data stored on the disk remains inaccessible to thieves and hackers.

FDE differs from File-Level Encryption (FLE) in that it secures all data stored on your hard drives automatically and transparently – including swap files and hidden files that may contain confidential data – without any user intervention. In contrast, FLE only protects specific files that are manually encrypted, and generally depends on the user to perform some action to ensure that files are encrypted before storage.

One drawback of FDE is that it does nothing to protect files "in motion." Once a file is sent via email or copied to a memory stick, it is no longer encrypted. For that reason, you may want to consider deploying FLE in conjunction with FDE, so that users have the option to manually encrypt files that need to be shared with others.

Most FDE products allow administrators to enable users to provide the encryption key for a system at the pre-boot stage in several ways:

- in the form of a password or passphrase;
- by inserting a USB drive containing the key;
- using a one-time password generating device such as an RSA token;
- using some biometric device such as a fingerprint reader (usually connected to a Trusted Platform Module which holds the actual encryption key.)

With many systems, administrators can also specify more than one authentication method, thereby creating a two factor authentication system.

Modern encryption algorithms, when implemented in a Federal Information Processing Standard (FIPS) 140 compliant manner, make it impractical – effectively impossible – for anyone to decrypt data on a drive using FDE without the key. That means that if a user loses or forgets their passphrase, the data on the encrypted drive will be permanently inaccessible unless the encryption part of the FDE product works with a key management system which enables key retrieval – either through a self service system or via a help desk.

FDE systems involve some processor (and therefore power) overhead to carry out the on-the-fly encryption and decryption, and the impact of this depends on the amount of disk I/O that individual applications demand. For users carrying out typical email and office productivity activities, the performance impact is unlikely to be noticeable – but it can be significant for very data-intensive activities such as video processing, unless the computer's main processor and the FDE product both support Intel's AES-NI instructions for hardware accelerated encryption and decryption.

Vulnerability to Attack

No security system is 100 percent secure, and FDE systems can be vulnerable to various attacks including:

Related Articles

Review: mobilEncrypt Cloud Based Encrypted Email
By Paul Rubens
July 27, 2011

- *Accessing the encryption key.* When users store a USB drive containing the encryption key along with a computer, accessing the encryption key becomes trivial for a thief. Users can also be fooled into revealing their password through social engineering.
- *Theft of the laptop while it is running.* FDE only protects data when the computer is turned off. That means that if a laptop is stolen while it is running but unattended (or while the user is distracted) the data will be fully accessible to the thief.
- *Advanced in-memory techniques.* FDE systems require that the encryption keys are held in memory while the system is running. Since the contents of DRAM chips persists for a period of seconds to minutes after a system is shut down, (and this time period can be extended by chilling the DRAM with canned air), it is possible to cut the power to a laptop that has been left unattended and boot it from a memory stick or CD into another operating system and read (and save) the contents of the DRAM. The key can then be extracted from this data and used in a subsequent attack.

It's also worth noting that some software applications place information on the main drive's boot sector, and this can get overwritten by FDE systems, causing them to stop working.

Overview of Leading Full Disk Encryption Products

Key things to look for when evaluating a FDE purchase are:

- Operating system support
- Authentication methods
- Key management systems and recovery options
- FIPS-140 compliant encryption modules
- Support for Intel AES-NI instructions

Here's an overview of some of the leading FDE vendors:

Check Point Full Disk Encryption. Check Point's FDE product works with Windows, Linux, and OS X. Multi-factor authentication options, such as certificate-based Smartcards and dynamic tokens, are supported.

The FDE system can be centrally managed by Check Point's Endpoint Policy Management Software Blade, enabling central policy administration, enforcement, and logging from a single console. Remote password change and one-time login remote help options are available for users who may have forgotten their passwords or lost access tokens.

McAfee Endpoint Encryption. Available for Windows and OS X, McAfee's Endpoint Encryption product provides full-disk encryption with support for AES-NI hardware acceleration.

McAfee ePolicy Orchestrator (ePO) management infrastructure provides centralized deployment, management, shared policy administration, password recovery, monitoring, reporting, auditing, and proof of protection. Access control includes two- and three-factor, pre-boot authentication.

Microsoft BitLocker Drive Encryption. BitLocker is included in the Ultimate and Enterprise versions of Windows 7, but not in the lower end versions. Once BitLocker is turned on, all files saved to the internal hard drive are encrypted automatically. It can also be used to encrypt external storage devices such as USB drives, using a feature called BitLocker To Go.

BitLocker can use an enterprise's existing Active Directory Domain Services (AD DS) infrastructure to remotely store recovery keys. The system provides a wizard for setup and management, as well as extensibility and manageability through a Windows Management Instrumentation (WMI) interface with scripting support. BitLocker also has a recovery console integrated into the early boot process to enable the user or helpdesk personnel to regain access to a locked computer.

Sophos SafeGuard Enterprise. Sophos's FDE product is available for Windows and OS X, and supports AES-NI instructions. It supports pre-boot user authentication with a password, token, smartcard, biometrics or key ring, as well as corporate Single Sign On (SSO) systems. Sophos' key management system provides recovery options for keys, data and forgotten passwords.

Symantec PGP Whole Disk Encryption. Available for Windows, OS X, and Linux systems, Symantec's PGP Whole Disk Encryption supports AES-NI instructions in all three operating systems when available. Users can authenticate using smart card, Trusted Platform Module (TPM), or passphrase.

Protected systems can be centrally managed by Symantec's PGP Universal Server – simplifying deployment, policy creation, key management, and reporting. Passphrase and machine recovery options include local self-recovery with question and answer authentication, and one-time-use tokens.

TrueCrypt. This free, open-source full disk encryption software is available for Windows, OS X, and Linux. It also supports AES-NI instructions.

TrueCrypt's main benefit is that it is free, which may be appealing to owners of very small businesses. However, it includes no key management system, so if a passphrase gets forgotten then there is no way to decrypt and access a drive. This shortcoming makes it unsuitable for use in anything but very small implementations.

WinMagic SecureDoc Disk Encryption. WinMagic's software provides FDE for Windows, OS X, and Linux. Pre-boot authentication is carried out using password, tokens, smartcards, biometrics and SSO systems.

SecureDoc is available in a standalone version, or as part of a centrally-managed whole disk encryption solution deployed from SecureDoc Enterprise Server (SES). SES provides a console that enables the configuration of users, groups, and profiles as well as key management, with integration with Active Directory.

Key management with SecureDoc is achieved using an encrypted database to store/escrow all keys for encrypted endpoints managed by SES. In the event of lost tokens or forgotten passwords, self-help and/or helpdesk-based challenge-response options enable password recovery.

Paul Rubens is an award-winning technology journalist who has been covering IT security for over 20 years. He has written for leading international publications including The Economist, The Times, The Financial Times, The Guardian, the BBC, and Computing.

22 Comment(s)

For secure email on the go, this type of app from Echoworx can really save the day but there are a couple of holes to sidestep.

» **Read Article**

- **AppSense Releases Free Dropbox Encryption App for iOS**
  By Pedro Hernandez | February 27, 2012
- **Passware Cracks Apple's FileVault Encryption**
  February 06, 2012
- **California DCSS Suffers Security Breach**
  March 30, 2012

Most Recent Mobile Security Articles

- Mobile Device Management: The Buying Basics
  August 22, 2014
- How to Detect SSL Leakage in Mobile Apps
  August 13, 2014
- Dude, How Secure Is My Connected Car?
  August 04, 2014
- How Microsoft Handles BYOD
  July 22, 2014