Data Protection Considerations

WRIGHT STATE UNIVERSITY

Contents

The following list identifies all the practices that should be implemented for protected data.

A. Workforce Identity and Account Management
B. Information Management
C. Continuity Planning and Disaster Recovery
D. Electronic Mail
E. Server Locations
F. Remote Access
G. Information for Users
H. Considerations

A. Workforce Identity and Account Management

1. Determine which individuals are authorized to work with ePI (Electronic Protected Information)
2. Establish security training for all members of the WSU workforce who are involved in the creation, transmission, and storage of ePI. Ensure that training program includes periodic security reminders and is updated to take into account current vulnerabilities and threats
3. Take disciplinary action in accordance with University personnel policies and guidelines on workforce members who fail to comply with University policy and procedures, including information security policy and procedures
4. Ensure the verification of the individual or entity who is authorized to access ePI and that the identity is correctly bound to a unique user identification ("log-on") for access to ePI
5. Ensure appropriate access controls mechanisms for authorized users' access to any ePI. For systems with the capability, require strong electronic authentication, such as sufficiently complex passwords or use of other encryption key mechanisms to access systems containing ePI.
6. Establish account maintenance procedures that ensure termination of accounts or change in access privileges for individuals or entities who have terminated or no longer are authorized to access ePI
7. Carefully manage system administrator accounts to ensure the accounts are used for only specific system administration functions. The number of these accounts should be kept to a minimum and provided only to personnel authorized to perform identified functions. Passwords or other authentication measures should be changed upon the termination of systems personnel who accessed these accounts
8. Log activities performed by system administrator accounts and monitor logs on a regular basis

B. Information Management

1. Identify relevant information systems
2. Ensure that agreements with third parties contain language that University ePI receive appropriate safeguards
3. Conduct risk assessments to identify the electronic information resources that require protection, and to understand and document risks from security failures that may cause loss of

confidentiality, integrity, or availability. Risk assessments should take into account the potential adverse impact on the University's reputation, operations, and assets. Risk assessments should include analysis that may result in modification of ePI by unauthorized sources

4. Select appropriate mechanisms to safeguard data relative to the sensitivity determined by the risk assessment. Procedures should address risks to integrity of ePI resulting from unauthorized access
    a. Systems containing ePI need to be hardened against known operating system vulnerabilities
    b. Where appropriate, install firewalls and intrusion detection software to reduce threat of unauthorized remote access
    c. Protect restricted data with appropriate strategies, such as removal of restricted data from data sets, secure file transfer, and use of web browser security standards, virtual private networks, and encryption
    d. Protect all devices against malicious software, such as computer viruses, Trojan horses, spyware, etc.
    e. Use change management practices for systems containing ePI
    f. Run versions of operating system and application software for which security patches are made available and installed in a timely manner on networked devices
5. Implement procedures to ensure regular review of login attempts and system activity, including the report of discrepancies
6. Where possible, terminate electronic sessions after a period of inactivity
7. Thoroughly scrub all ePI from any storage media prior to disposal or re-use
8. Implement appropriate logical security measures, such as encryption, to protect data from unauthorized access if systems or work-stations containing ePI cannot be housed in a managed secure location, i.e., data center
9. Conduct back up of data and software on an established schedule. Back up copies should be stored in a physically separate location from the data source

C. Continuity Planning and Disaster Recovery

1. Ensure that business continuity planning includes measures to enable continuation of critical business processes while operating in emergency mode and to recover from a disaster that renders resources unavailable for an acceptable period of time. Disaster recovery plans must be tested on a periodic basis or in response to major changes to the working environment
2. Continuity plans must undergo periodic testing and revised as appropriate
3. Establish procedures to ensure that ePI can be accessed during an emergency

D. Electronic Mail

1. Inform all users about the risks of email and adopt programs to educate staff regarding appropriate use of email
2. All confidential email must be sent via secure channels
3. Whenever deemed necessary and possible encrypt transmissions containing ePI

E. Server Locations

1. Server locations that contain ePI should be located in professionally-managed secure locations that have provisions for prevention, detection, early warning of, and recovery from emergency conditions created by earthquake, fire, water leakage or flooding, power disruption, air conditioning failures, or other hazards
2. These secure locations must have physical access controls, such as locks, electronic key readers, or other access control mechanisms
3. Record any maintenance repairs and modifications to physical components of the facility related to security, such as hardware, walls, doors, and locks
4. Record relocation of hardware and electronic media. Assign responsibility for maintaining records of hardware and software
5. Limit access to secure locations to authorized users only, and maintain logs to track ingress and egress from location
6. Ensure back up of data before the relocation of equipment

F. Remote Access

1. All remote access into WSU networks must be by secure methods only, such as authorized VPNs
2. Storage of ePI on any non-university equipment is forbidden unless formal exemption granted following assessment of the risks
3. Since laptops can never be adequately secured physically the best protection is encryption that would render the laptop contents undecipherable to unauthorized users

G. Information for Users

1. All members of the WSU workforce who are involved in the creation, transmission and storage of ePI must receive training about the security rule
2. Access to ePI is limited to those individuals for whom it is an authorized work related requirement
3. You may be subject to disciplinary action in accordance with University policies and guidelines on individuals who fail to comply with security policy and procedures. Misuse or unauthorized access of ePI may be subject to sanction and disciplinary actions
4. You must use a sufficiently complex passwords to access systems containing ePI. Passwords must never be shared. Passwords should be developed in accordance to policies set by campus information technology (CaTS) services.
5. You must run versions of operating system(s) and application software that have security patches available and installed in a timely manner.
6. All devices must be protected against malicious software, such as computer viruses, Trojan horses, spyware, etc. Where appropriate, firewalls and intrusion detection software reduce threat of unauthorized remote access. This includes servers, workstations.
7. Portable devices, such as laptops, if they contain ePI must be password protected or encrypted, and other logical controls installed, since they cannot be physically secured.

8. All devices that contain ePI must be backed up on an established schedule.
9. You must secure, maintain and when necessary dispose of all removable electronic media that may contain ePI according to established procedures.
10. Whenever required, encrypt electronic transmissions containing ePI (such as email). If encryption is not available, consider email a public document.

Considerations

Audit Retention

The rule requires that records be maintained of “activity in information systems that contain or use ePI.

Requirements - Time Limit The requirement for retention is for six years. It would be prohibitively expensive to store massive amounts of data for years.

Only logs relevant to security incidents should be retained for six years and the remainder of the data should only be retained for up to 90 days in accordance with usual and customary practice.

Periodic audits should be conducted of the information systems so that relevant audit logs can be identified for future review even if no incident has come to light.

Email Encryption

Electronic mail is fundamentally insecure. Unencrypted mail in transit may potentially be viewed by many individuals since it may pass through several switches enroute to its final destination. It may not reach the intended recipient at all. In practice the risks for a single piece of email are extremely small given the volume of email traffic. Emails containing ePI need a higher level of security. The following recommendations are offered to address these concerns:

1. Educate staff about the limitations of email. Any solution will depend on changing behavior and attitudes to the use of email
2. Implement an email encryption program and train staff how to use appropriately

Patch Management

Protection from security breaches in large part depends on computing system maintenance. Software vendors regularly provide updates or patches so that their products continue to be valuable to their customers. Ensuring that all available and relevant patches are installed is an ongoing and complicated activity. In addition maintaining anti-virus and anti-spyware programs is a continuous challenge. In most network environments the managers can ensure that computers on the network are running the correct versions and have installed patches. Computers that may not be on the network such as laptops and PDAs will require more active surveillance and maintenance by the individual users.

Physical Security

Data must be available when needed but its integrity must be maintained. Access to systems containing ePI must be controlled as carefully as possible. Computers that are located in insecure locations and/or accessed by contract cleaning and maintenance services need to be carefully secured. Record any maintenance repairs and modifications to physical components of the facility related to security, such as hardware, walls, doors, drop ceilings and locks. Limit access to secure locations to authorized users only, and maintain logs to track ingress and egress from location.

Servers containing ePI should be housed in secure locations that have solutions for prevention, detection, early warning of, and recovery from emergency conditions created by earthquake, fire, water leakage or flooding, power disruption, air conditioning failures, or other hazards.

Secure locations must have physical access controls, such as locks, electronic key readers, or other access control mechanisms. Physical security is very often difficult to maintain in unsupervised open areas. Desktops and laptops are by definition not housed in secure areas so ePI should be stored on a network server is available. Wireless networks and signals should be encrypted and access points hidden.

Backing Up/Contingency Plans

Any equipment containing ePI should be regularly backed up to preserve the availability and integrity of the data. Contingency plans for a disaster should take into account the need to restore data in a rational manner. Adequate contingency planning would be based on the criticality of the data, how frequently it is accessed and how quickly it is needed. Paper backup methods should be devised if appropriate. The availability of equipment to which to restore lost data must also be assessed. Back up strategies should take into account not only disaster recovery needs, but also routine departmental workstation or system back up needs. Damage to systems can be widespread and therefore machines and data for recovery purposes must be in physically separate locations. If this is not possible then use of equipment such as fireproof safes are recommended. Replacement equipment can be drop shipped on a pre-arranged basis. Data stored on mobile devices should be considered so vulnerable that the essential contingency plan for such data should be the presumption that it will be lost at some point.

Remote Access

Use of portable devices and home computers to access ePI remotely is inherently insecure and requires solutions within a framework of strict access controls. Storage of ePI on any home computer is against University policy. Laptops can never be adequately secured physically so the best protection is data encryption. The laptop contents would be undecipherable to unauthorized users. PDAs should be set up to require login that cannot be disabled by the user. All data on PDAs should be regularly synchronized with servers so that if a PDA equipped with login is lost or the password is lost then no data will be recoverable. Some devices such as the Blackberry™ can be set to permit only 10 login attempts before erasing all data. Publicly accessible computers, open wireless networks and third party proxy services (Yahoo!, Hotmail, etc…) are all very vulnerable to penetration by malicious software and hackers and access to ePI via such systems should be discouraged strongly. Virtual Private Networks (VPN) should be required. Along with this requirement comes the obligation to maintain security patches at remote locations.

Password Management

Passwords are one of the most universal and widely distributed forms of computer security, without individual and sufficiently complex passwords systems containing ePI cannot be secured. Strong passwords include numbers, symbols and letters of different cases. Since these type of passwords can be difficult to recall the use of an acronym is advisable. Biometric identification devices and token based systems should be seriously considered as they become available, viable and cost effective.

Automatic Logoff

Equipment and some software programs are designed to log users off after a predetermined period of inactivity, either are adequate.

Termination Procedures

Systems must automatically terminate access to ePI data.