

Working with Sensitive Data – Some Guidelines

Jamie Sonsini

Information Systems & Computing

October 2009

Some elements of data are more sensitive than others. In the wrong hands, specific data can provide the necessary information to allow a person to masquerade as another (identity theft). Several kinds of information are protected by law and require careful handling. We refer to this information as “sensitive data.”

The following document, an update to one I shared with you 3 years ago, attempts to offer some guidelines for working with such data.

I. Do You Have Sensitive Data?

Data as described below must be handled properly, by only those who need access to carry out their University duties, and must be disposed of properly.

A. Electronic Protected Health Information (ePHI)

The Health Insurance Portability and Accountability Act (HIPAA) defines electronic protected health information (ePHI) as any electronic information that is created or received by a health care provider that relates to the past, present, or future physical or mental health of an individual and that identifies the individual.

B. Personal Information

Personal information may be defined as first name (or first initial) and last name in combination with one or more of the following:

- a) Social security number,
- b) Driver's license number,
- c) California identification number,
- d) Personal health information,
- e) Health insurance information,
- f) Financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

C. Family Educational Rights and Privacy Act Information

The Family Education Rights & Privacy Act (FERPA) is federal legislation that affects the way Universities administer student information and protects the privacy of student educational records.

II. Personal Practices

A. General – Best Practices

1. Password protect all workstations, especially those with sensitive data or used to access such information.
2. Don't share computer accounts with others.
3. Notify your department management that you are in possession of sensitive data.

4. If sensitive data must be shared, be sure you have a safe conduit for this exchange of information.
5. Consider physical access to your office. Special care must be taken if your office is an open cubicle.
6. If sensitive data is stored on removable media (floppy disk, CD, tapes, etc.) do not leave these items lying around your office. They should be stored in a secure and protected location.
7. Employ safe practices when using your personal computing devices (e.g., desktop systems, laptops, PDAs, smart phones, etc.). For example:
 - a) Keep your software up-to-date.
 - b) Run anti-virus and anti-spyware software.
 - c) Be careful when browsing the web, downloading programs and opening e-mail attachments. Sources of unsolicited information, such as advertising pop-ups and spam often contain links to malware and should be avoided.
 - d) Use a password with your screen saver.
 - e) Turn off your computer when it's not in use.

B. Passwords – Best Practices

1. Access to data repositories and services is usually granted after providing an identifier (sometimes called a “user ID”) and a password. Special care must be taken to select a password that would be hard for others to guess (even if they use clever computer programs to do their guessing).
2. You should know who (besides yourself) is able to change your password. Typically, someone responsible for managing network services (the “system administrator”) would have such privileges.
3. Many computer systems will offer to save userids and passwords used to access a particular service. This is intended to be a convenience. Avoid saving any userid or password used to access sensitive data. If such information was saved, access to this information would be easily obtained by anyone who has physical access to your workstation.
4. Passwords should:
 - a) Be changed every 6 months,
 - b) Have a minimum of 6 alphanumeric characters,
 - c) Contain a mix of at least one numeric and one alpha character,
 - d) Not be reused within 8 changes,
 - e) Not be words found in the dictionary.

C. Inadvertent Exposure

1. If you have sensitive data displayed on your computer monitor, you should be careful not to expose this information to others visiting your office or work space. Closing or minimizing the application displaying the information, using a screen saver or actually locking your computer are all effective means to avoid this risk. Of course, if you actually leave your office while using sensitive data, special care should be taken and your workstation should be “locked.”

2. Papers with sensitive data should also be carefully handled and not left lying around so as to be read by an office visitor. If documents containing sensitive data are no longer needed, they should be shredded (and not simply tossed into the recycle bin). This caution should be extended to CD's, removable disks, tapes, or computing equipment that is to be discarded.
3. Special care should be taken to remove all data from an old computer being replaced.
4. If you print a document that contains sensitive data, don't leave it where others may view the information.
5. If you are printing a document that contains sensitive data and the document does not print, make sure you have properly cancelled this task. Taking such precautions avoids the risk of your document printing at a later time and exposing this information to others using the printer.

III. Departmental Considerations

A. Who needs to handle sensitive data?

1. The department should be able to identify those members responsible for handling and storing sensitive data and should monitor changes to those responsible for these duties.
2. The department should also know with whom outside of the department this information is shared.

B. Is data necessary to conduct departmental business?

1. Care should be taken that the use of sensitive data is restricted to its defined purpose.
2. The department managing sensitive data should consider alternate methods and procedures which do not involve storing or handling sensitive data. If such data elements are not truly needed, their use should be avoided. For example, using a Social Security Number as an identifier only because it is unique may be a poor choice. Other identifiers, such as our employee ID number, are unique and are not considered sensitive data.

C. Training

The department should include information and directions on handling and storing sensitive data in any training provided to new employees. These procedures should be periodically reviewed by all department staff.

IV. Data Handling

A. Storage (Server or Workstation)

1. In general, sensitive data should not be stored on an individual workstation. If it must, however, this device should be well protected from intrusion and backed up regularly. Since these requirements are often difficult for an individual workstation, it is recommended that sensitive data always be stored on a well managed file server system.
2. If sensitive data is stored on a computer system, the frequency of that system's backups and the process for requesting a restoration of data (should data be damaged or erased) should be well understood.
3. You should understand who else has access to the system in question and what protections are available.

B. Computers at Home, Traveling Laptops, Handheld PDAs

1. Special thought should be given to avoiding the storage of sensitive data on any portable device. These devices, such as laptops or PDAs, are easily stolen or misplaced. The presence of sensitive data turns an inconvenience into a serious matter.
2. If, for operational reasons, sensitive data must be stored on a portable device or portable media (tape, memory stick, CD, etc.) this data should be encrypted. This is especially important since these items are small and easily lost or stolen. Encryption offers the best protection against such loss or theft and their consequences.

C. Encryption

There are various options for protecting data by employing encryption technology. You should work with your Information Technology support staff to determine the suitability of any solution.

1. Individual applications (e.g, MS Office) may have document encryption available.
2. Various software vendors offer encryption schemes that involve Public/Private keys.
3. Newer versions of the Windows and Macintosh operating systems provide features that allow for encrypting files, folders or entire disk drives. Care must be taken when using such powerful features, since missteps can remove all access to the encrypted information.
4. Some applications (e.g, MS SQL 2005) allow you to encrypt specific data elements. This can be quite useful if the data source has some fields which are sensitive and others which are not.

V. Sharing with Others

Before sensitive data is shared with others, thought should be given to the necessity of this sharing. Any means of sharing data does, automatically, introduce opportunities for the data to be exposed to or used by others who might not maintain the necessary security.

A. Sharing Accounts and/or Workstations

Special care should be taken to avoid storing sensitive data on accounts or workstations that are shared, or accessible, to others. This sharing decreases the security of this data.

B. Sharing via Email

1. Inherently, Email is a non-secure means of communication. There are several reasons for this:
 - a) In general the contents of an email message are communicated in “clear text”. This means that anyone “snooping” the network over which the email travels could actually view the email contents.
 - b) Once you have sent an email message to another person, you have no knowledge of what that person might do with this email message. They could forward a copy of your email to someone else who may not be authorized to view the information contained in the email message. Once it leaves your desk, it’s out of your control.
 - c) Email can be forged. You may receive an email message appearing to be from one person, but in fact it could have come from someone else attempting to fool you. Phishers, hackers and spammers do this all of the time. Be especially

cautious with email requests for information. Responsible organizations will not request sensitive information through email.

d) Watch for automated processes that generate email.

With these reasons in mind, it is prudent to avoid sharing sensitive data via email.

2. If an email message must contain sensitive data it would be wise to encrypt the email message contents. Several products and schemes exist that provide this feature.

C. File Sharing

1. If sensitive data is to be shared (on a file server, for example) care should be taken so that only those needing access have it.

2. If sensitive data must be stored and shared with others, consideration should be given to encrypting the data. Only those authorized to work with this data should then be able to view it.

3. If sensitive data is shared the other party should be notified that the data is sensitive and will require special handling.

VI. A Final Note

If you believe that sensitive data has been exposed, lost or stolen contact your local Information Technology support staff and notify your department management immediately.

If you have questions about sensitive data or security, you may contact Karl Heins, Chief Information Security Officer, Office of Information Technology (Karl.Heins@oist.ucsb.edu or X8843).