Risk Assessment—Inventory Checklist for Sensitive / Confidential Information

Step 1:

What type of information are you trying to protect? This is a decision that each organization makes in light of their business, regulatory requirements, etc. At a minimum, the data to be protected should include:

- An individual's first name or first initial and last name
- Social Security Numbers; driver's license number or state card numbers
- Financial account numbers; credit or debit card numbers;
- Security codes, access codes, or passwords (e.g., a PIN) related to an individual's financial accounts, credit/debit cards;
- Medical information (any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional);
- Health insurance information (an individual's health insurance policy number or subscriber ID number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records).

Other information that you should consider protecting includes customer information, such as:

- Taxpayer records
- Customer Transaction Information, like order history, account numbers, etc.
- Financial information, like account balances, loan history, and credit reports
- Email addresses, passwords, phone lists, and home addresses (while may not be independently sensitive, may be more sensitive with one or more of the above data elements)

Or information related to business partners, like:

- Vendors and business partners may provide some of the above information, particularly for Sub-contractors and Independent Contractors
- All of the above types of information may also be received from commercial clients as a part of commercial transactions or services
- Financial / sales projections, forecasts, M&A activity, and trade secrets

Step 2:

After you identify what information you plan to protect, you must know where these sensitive and confidential data are located. This checklist helps you identify places and equipment where you might find sensitive and confidential information. This list should help you think in broad terms about where to look for sensitive / confidential data.

This list includes devices that may pose a risk of unauthorized use/disclosure of sensitive data even if they do not directly contain the protected data. For example, a smartphone with a server password stored in its "contacts" could allow someone into the network if an individual steals the smartphone. Also, consider items stored away from the office such as a flash drive at a worker's home because these devices should also be evaluated for potential risk.

<u>DEVICES</u>

- Computers
- Laptops
- Tablets
- Servers
- External Storage Arrays (e.g. Dell MD-3000)
- Network-Attached-Storage (NAS) devices
- Smartphones

- Cameras
- Voicemail Recordings
- Routers
- Video Surveillance System
- Reader Devices (e.g. Kindle)
- Music Players (e.g. iPod, mp3 player, etc.)
- Digital Copy Machines
- Scanner with a Storage Drive
- Fax Machines
- Phones (e.g. if phone numbers are logged)
- Medical Devices with Local Storage (e.g. ultrasound machine, MRI machine, etc.)
- Future Devices Not Yet on the Market
- Any Other Device that may Store or Allow Access to electronic data

OFFLINE MEDIA

- Compact Discs (CD-ROMs, such as copies of radiographs)
- DVDs
- Thumb Drives, a.k.a. Flash Drives
- External Hard Drives such as USB, eSATA, or Firewire
- Backup Tapes
- SAN Disks (e.g., storage for cameras)
- Smart Cards (used for secure log-in in some organizations)
- Encryption Keycards
- Door Keycards
- Floppy Disks
- Iomega Disks
- Hard Drives (e.g. secondary backup drives or stored hard drives from old computers)
- Any Other External Media Type

OFF-SITE SERVICES

- Off-site Backup Servers
- Off-site Hosted Services
- Websites
- FTP Sites
- E-mail Spam Filtering Services
- Web Filtering Services
- Any Other Off-site Service that may be Relevant

DATA IN TRANSMISSION

- Internal e-mail
- External e-mail
- FTP
- Web Traffic
- WebDAV
- Peer-to-Peer File Sharing
- File Sharing (LAN-based, such as between workstations and a server)
- SQL or Other Database Traffic
- Any Other Type of Data Transmission

REMOTE ACCESS

- Webmail
- POP3 e-mail

- IMAP e-mail
- Outlook Anywhere e-mail
- ActiveSync e-mail Synching to a Phone
- BlackBerry Enterprise Server
- Remote Desktop
- Terminal Server
- VPN
- GoToMyPC
- LogMeIn
- TeamViewer
- PCAnywhere
- VNC
- Web portal
- Any Other Type of Remote Access