Purpose of This Guide

Following the HHS/OCR Final Guidance on Risk Analysis and National Institute of Standards and Technology (NIST) SP800-30 Revision 1 Guide for Conducting Risk Assessments Clearwater performs, and recommends Customers perform, risk analysis at the level of **each information asset used to create, receive or store or transmit** sensitive information. There can be a wide variation in the number of assets from one organization to the next. This guide is intended to assist organizations in thinking about how information assets should be identified, inventoried and analyzed.

What's On Your Balance Sheet?

Traditional definitions of an *asset* are:

- "…a useful or valuable thing, person, or quality…"
- "…an economic resource…"
- "…anything tangible or intangible that is capable of being owned or controlled to produce value and that is held to have positive economic value…"

Common definitions of an *information asset* include:

- "…any data, device, or other component of the IT environment that supports *information management*-related activities …"
- "… a body of knowledge that is organized and managed as a single entity…"
- "…an identifiable collection of data stored in any manner and recognized as having value for the purpose of enabling an organization to perform its business functions, thereby satisfying a recognized business requirement*."*

Like any other corporate asset, an organization's information assets have business value. Since information assets, unlike physical assets, do not often appear on the organization's balance sheet, identifying information assets can be a source of confusion.

The Clearwater Compliance definition of an information asset which should be considered within the scope of an organization's information risk management program, is:

> ***A business application, system or solution that creates, receives, maintains or transmits sensitive information, such as Protected Health Information (PHI), personally identifiable information (PII), payment card data, company proprietary business plans or financial data, etc., the confidentiality, integrity and availability of which must be safeguarded for the sake of overall business risk management.***

Unlike traditional hard assets, like desktop computers, laptops, and servers, information assets in this context are not necessarily physical, individual, "things" that might bear an "asset tag". Rather, they are software applications, integrated devices, and third party services used to access, create, transmit, maintain, or receive sensitive data of interest (e.g. PHI, PII, payment card data, billing/financial information, payroll information, etc.). More about each type of information asset follows below.

Software Applications – NIST defines an information system as "…a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." A software application defines or performs the functionality of the information system. Thus, software to be included in your Information Asset Inventory might include : electronic health record applications, clinical information applications, lab and/or medical specialty applications, medical billing/claims processing applications, email applications, company intranet websites, HR management applications, network file sharing applications, EDI applications, fax

applications, payment processing applications, financial management/reporting applications, and any other software used to manage sensitive electronic information. It does not matter if these applications were internally developed, purchased off-the-shelf, or hosted by your organization or hosted on a third party's computer hardware (i.e. Platform-as-a-Service or Software-as-a-Service).

Integrated Devices or Equipment **--** Certain types of devices or equipment which are used to create, receive, maintain or transmit sensitive information perform very specialized functions, and the software and hardware are integrated in such a manner that neither will work without the other. Examples of the type of integrated devices or equipment you might include in your Information Asset Inventory are multi-function printers, copiers, fax machines, closed-circuit TV recording equipment, laboratory equipment (e.g. blood gas analyzer), medication or medical supply cabinets, and radiological equipment (e.g. X-ray machines, CAT, PET, or MRI scanners, etc.).

Third-party Services – Most-often missed in thinking about risks to information assets are third party vendors engaged by your organization in some capacity that requires them to create, receive, maintain or transmit your sensitive information. Because of the access these third parties have to the organization's sensitive information, it is vital that the risks posed to the confidentiality, integrity and availability of your sensitive information by that third party also be evaluated. Thus, they should also be included in your Information Asset Inventory. Examples include, but are not limited to: Platform-as-a-Service providers (often cloud-based), software suppliers (including Software-as-a-Service providers), hardware maintenance services, backup media management companies, HR/benefits services, payroll services medical transcription services, medical coding processors and all other hired consultants/contractors having regular access to your sensitive information.

Where Does the Sensitive Information Actually Live?

Information assets create, receive, maintain or transmit information using one or more types of storage media, or simply *media* for short. While this includes physical storage media, such as backup tapes, CD/DVD disks, USB drives, and SD cards, it also includes devices that contain some form of permanent electronic storage, like hard drives, thumb drives, CD-ROM/DVDs. Devices with this form of non-volatile storage include desktop and laptop computers, servers, storage area networks, network attached storage, smartphones, and tablets, and multifunction scanner/printer/copier devices.

Understanding and identifying all the storage media which host sensitive information is ultimately critical to understanding all the potential compromises to the confidentiality, integrity and availability of that sensitive information. However, at Clearwater, for the purpose of developing fixed-price quotations for conducting comprehensive NIST-based risk assessments, the initial focus should be on identifying and inventorying all the discrete information assets as defined above and NOT necessarily the underlying media.

Whether Clearwater or the customer performs the NIST-based risk assessment, the methodology and Clearwater IRM|Analysis™ software facilitates the classification and documentation of all information assets and media. Clearwater's software provides capability to classify media into *media classes* with similar threat surfaces to simplify risk assessment and, ultimately, risk response action planning. The use of media classes greatly reduces the effort in performing a NIST-based risk assessment while maintaining the integrity of the overall NIST risk management process and approach. Detailed threat identification, vulnerability analysis, controls evaluation and risk valuation is greatly simplified. Summarization of risks in the risk register, risk response planning and risk monitoring is further simplified through the use of media classes.

Asset Example Lists – By Organization Type:

The types of information assets any organization might have varies based on the nature of the business and the services provided. By way of thought stimulation, and with no intention of providing an exhaustive list, below are some information assets that might be present within various types of organizations.

+ If your organization is a Health System / Hospital, your Information Asset Inventory would likely include, but not be limited to these information assets:

- Automated Medication or Medical Supply Cabinets
- Administrative Workstations (e.g. Desktop and Laptop Computers)
- Billing Information System
- Claims Payment System
- Clinical Workstations (e.g. Thin or Zero-client Computers, Portable Laptop Carts, etc.)
- Closed Circuit Television (CCTV) System
- Core Health Information System
- Diagnostic Equipment (e.g. EKG, EEG, Pulmonary Function Testing, etc.)
- Laboratory Equipment (e.g. Hematology Analyzer, Coagulometer, Cell Counters, etc.)
- Radiological Equipment (e.g. CT , MRI and PET Scanners; Mammography, Ultrasound and X-Ray Machines; Gamma Knife; etc.)
- Document Management System
- Electronic Health Record System
- Emergency Department System
- Email System
- Fax System
- Financial System
- Lab Information System
- Network File Shares
- ICU/NICU Telemetry System
- Oncology System
- Operating Room Software
- PACS System
- Radiology Information System
- Microsoft SharePoint
- Incident Management System
- Document/Records Storage and Management Vendor
- Medical Equipment Maintenance Supplier

Special Note for Hospitals - It should be observed that often one integrated Hospital Information System may provide many of the functions listed above within separate modules of the same application or information asset. If one set of security controls is in place for that integrated system, it should be considered one asset. Hospitals may also utilize a variety of medical devices that should be classified rather being listed individually. Informed Information Risk Management indicates that priority should be placed on devices with Network or WiFi capability over devices that are isolated from the network or internet.

+ If your organization is a HIPAA Business Associate, your Information Asset Inventory would likely include, but not be limited to these information assets:

- Customer Relationship Management System
- Financial Management and Reporting System
- Billing System
- Data Warehouse
- Email System
- Network File Shares
- Proprietary Information System
- Microsoft SharePoint
- IT Services Provider

+ If your organization is a commercial Health Plan, your Information Asset Inventory would likely include, but not be limited to these information assets:

- Authorization System
- Claims System
- Data Backup
- Data Warehouse
- Document Management System
- EDI Gateway
- Email System
- Exchange or Email System
- EOB Systems
- Fax System
- FTP System
- HEDIS Reporting System
- Member Portal
- Network File Shares
- Pharmacy Benefits Management System
- Proprietary Information System
- Provider Portal
- Microsoft SharePoint
- Document/Records Storage and Management Vendor
- IT Services Provider
- IT Equipment Maintenance Provider

+ If your organization is a self-funded Group Health Plan, your Information Asset Inventory would likely include, but not be limited to these information assets:

- Data Backup System
- Email System
- Network File Shares

- Microsoft SharePoint
- Fax System
- FTP System
- File Sharing
- Billing System
- Provider Portal
- SharePoint

+ If your organization is a Medical Practice/Outpatient Clinic, your Information Asset Inventory would likely include, but not be limited to these information assets:

- Clinical Information System
- Electronic Health Record System
- Fax System
- FTP System
- Billing System
- Email System
- Network File Shares
- Practice Management System
- IT Services Provider

+ If your organization is a Long Term Care or Hospice facility, your Information Asset Inventory would likely include, but not be limited to these information assets:

- Clinical Information System
- Billing System
- Email System
- Fax System
- FTP System
- Medication Management System
- Network File Shares
- Microsoft SharePoint

+ If your organization creates, receives, maintains or transmits payment card data and is subject to the Payment Card Industry Data Security Standard (PCI DSS), your Information Asset Inventory would likely include, but not be limited to these information assets:

- Clearing & Settlement Services
- Issuer Processing
- Payment Gateway
- Payment Application (app should be certified by PCI)
- Terminal Management System