Purpose of This Guide
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 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. 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.

Information Asset Definition
Common definitions of an information asset include:

- “... a major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.”
- “... any software, hardware, data, administrative, physical, communications, or personnel resource within an information system.”
- “…any data, device, or other component of the IT environment that supports information management-related activities ...”
- “…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.”

Consistent with other corporate assets, 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 them can be perplexing.

The Clearwater Compliance definition of an information asset, which should be considered within the context 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 industry (PCI) data, intellectual property (IP), 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. Information assets also include the increasingly greater number of technologies (hardware, software, networking devices, physical plant devices and biomedical devices) that are part of the Internet of Things (IoT) where compromise may result in loss or harm to the organization or to its patients.
The Clearwater Definition of an Information Asset
(with Examples for different organizations)

Categories of Information Assets to Consider for Risk Analysis

As more and more technology is designed and deployed in healthcare settings and more and more data is digitized, the categories of information assets that create, receive, maintain or transmit sensitive information and/or the equipment and devices that facilitate the processing of sensitive information continues to expand. Clearwater’s IRM|Analysis™ SaaS platform continues to evolve to include reasonably anticipated threat sources and threat events, vulnerabilities and controls that may be implemented to mitigate threats from exploiting vulnerabilities that may ultimately result in a compromise of sensitive data or equipment.

Following are categories of information assets that organizations must consider in their information risk management, compliance risk management and technical testing programs.

I. **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 is the executive process that binds these resources together into a functional system. Thus, software applications to be included in your Information Asset Inventory might include, but not be limited to:

- 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, hosted by your organization or hosted by a third party (i.e. Platform-as-a-Service or Software-as-a-Service).

II. **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. 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, physical cardkey security systems, HVAC systems, etc. These types of
assets should be grouped where possible into classes that have similar threat surfaces and controls. It is typically not a best practice to list individual pieces of equipment in your asset inventory for the purpose of information risk management.

III. **Medical Devices** – The FDA defines a medical device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:

✓ recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,
✓ intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
✓ intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes."

Medical devices range from simple tongue depressors and bedpans to complex programmable pacemakers with micro-chip technology and laser surgical devices. In addition, medical devices include in vitro diagnostic products, such as general-purpose lab equipment, reagents, and test kits, which may include monoclonal antibody technology. Certain electronic radiation emitting products with medical application and claims meet the definition of medical device. Examples include diagnostic ultrasound products, x-ray machines and medical lasers. Medical devices that are part of the IoT or create, receive, maintain or transmit ePHI or other sensitive data should be considered for inclusion in an organization’s information asset inventory.

Health care organizations must be especially mindful of the impact of cybersecurity threats to the integrity and availability of these medical devices. When critical diagnostic devices (i.e., PACS, CT, MRI, Vital Monitoring Systems, etc.) are compromised through malware attacks, these services are rendered inoperative and can impact patient care, organization revenue and reputation. Evaluating threats and vulnerabilities to these “information assets” is crucial to a complete risk analysis.

These types of assets should also be grouped where possible into classes that have similar threat surfaces and controls. It is typically not a best practice to list individual pieces of equipment in your asset inventory for the purpose of information risk management.

IV. **Third-party Services and Providers** – Many organizations often omit information assets that are hosted and/or managed by third party vendors and Business Associates (BA) under contract with the organization to create, receive, maintain or transmit sensitive information. It is vital
that the risks posed to the confidentiality, integrity and availability of sensitive information by a third party be evaluated because of their access to sensitive corporate information. They should be included in your Information Asset Inventory. Examples include, but are not limited to: Platform-as-a-Service providers (i.e., AWS, Azure, Google, Rackspace, etc.), software-as-a-service providers (i.e., Office 365, Google Docs, Press Ganey, etc.), hardware maintenance services, backup media management companies, HR/benefits services, payroll services medical transcription services, medical coding processors and all other consultants/contractors having regular access to your sensitive information.

V. **Networking Infrastructure Components** -- certain network components may create, receive, maintain or transmit ePHI or other sensitive information. A compromise of their integrity or availability could adversely affect access to care, timely care or quality of care. Clearwater is currently expanding its ability to conduct detailed network equipment risk analyses and will discuss the requirements and approach with you. Network components that may be considered for risk analysis and/or technical testing include, but are not limited to:

**Networking Hardware:**
- ✓ Routers
- ✓ Switches
- ✓ LAN cards
- ✓ Wireless routers
- ✓ Cables

**Networking Software:**
- ✓ Network operations and management
- ✓ Operating systems
- ✓ Firewall
- ✓ Network security applications

**Network Services:**
- ✓ Optical Switching
- ✓ Metro Ethernet
- ✓ MPLS
- ✓ Satellite
- ✓ Wireless protocols
- ✓ VPN solution
- ✓ IP addressing

**Network Security:**
- ✓ Active devices such as firewalls, antimalware scanning, content filtering, antispam, antimalware devices, data leak protection solutions
- ✓ Passive devices, such as intrusion detection appliances
✓ Preventative systems such as penetration testing devices, vulnerability assessment appliances, encryption solutions, 2FA solutions
✓ Unified Threat Management (UTM) appliances which serve as all-in-one security devices
✓ Active Directory
✓ Asset and Change Management solutions

VI. **Often-missed Information Assets or Media** – while organizations are required to identify where all sensitive information may reside, many organizations struggle to maintain an inventory of these systems and applications. The following list is designed to stimulate additional thinking about what other information assets should be included in the information asset inventory:

1. **Closed-Circuit TV system** for security at any site that stores the recorded images of patients
2. **Voice system** that stores messages or recordings
3. **Digital cameras / photography systems** at any site to take pictures of patient
4. **Pagers** that capture messages about patients
5. **Diagnostic equipment** (e.g. EKG, EEG, Esophageal cameras, etc.) which store both patient data
6. **Radiological modalities** which store both images
7. **Lab equipment** (e.g. blood analyzers, flow cytometers, etc.) which stores patient lab results
8. **Monitoring or telemetry devices** (e.g. vital sign monitors, Holter monitors, insulin pumps, etc.)
9. **Automated medication or medical supply cabinets** (e.g. Omnicell, Pyxis, Lynx Mobile, etc.)
10. **Third-party vendors** or consultants that do not provide “health care services”, such as transcriptionists, billing code review services, etc.
11. **Third-party collection services** to collect overdue patient bills
12. **Third-party file-sharing services** (e.g. DropBox, Google Drive, Microsoft OneDrive, etc.)
13. **Third-party data backup services** (e.g. CrashPlan, Carbonite, LiveVault, Mozy, etc.)
14. **Other third-parties** that access ePHI
15. **Stand-alone servers or shared workstations** at any site that store ePHI (e.g. act as network file shares)
16. **Stand-alone fax machines** that are used to transmit or receive documents with ePHI
17. **Stand-alone copy machines** that copy documents with ePHI
18. **Stand-alone scanners** that scan documents with ePHI
19. **Stand-alone multi-function devices (copiers, printers, scanners)** that print documents with ePHI
20. **External hard drives** connected to workstations (i.e. desktop PCs, laptop PC, etc)
21. **Flash drives, CDs, DVDs or other external media** made in response to a patient request for their medical records
22. **Legacy flash drives, CDs, DVDs, magnetic tapes or other external media** from legacy systems that are no longer in service

**Where Does the Sensitive Information Actually Reside?**
Information assets create, receive, maintain or transmit information using one or more types of storage media, or simply "media" for short. 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 deployed 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 sample information asset lists that might be present within various types of organizations.

I. Health System / Hospital - 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, TEG devices, 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. These modules will vary in workflow and security controls. An operating room EHR module will have extended time-outs due to surgical needs and may have unique sign-on exemptions. This is important in differentiating whether each module is treated as a unique asset or whether it can be grouped. Hospitals may 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.

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

• Business Associates core application or platform offering
• 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
III. Commercial Health Plan - 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

IV. Self-funded Group Health Plan - 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:

- ERP System
- Data Backup System
- Email System
- Network File Shares
- Microsoft SharePoint
- Fax System
- FTP System
- File Sharing
- Billing System
- Provider Portal
- SharePoint

V. Medical Practice/Outpatient Clinic - 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
The Clearwater Definition of an Information Asset  
(With Examples for Different Organizations)

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

VI.  **Long-Term Care Facility or Hospice** - If your organization is a Long-Term Care Facility or Hospice organization, 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

VII.  **Payment Card Industry Data** - 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