

Columbia University Medical Center
Application Security Documentation List for Tier A Assets
Version 4.0, April 1, 2005

All CUMC EPHI asset owners and systems must follow CUMC EPHI security policies.

Protected Health Information (PHI) is defined as health or medical information identifiably linked to a specific individual including Identity information (**demographic and financial data**) and medical condition and treatment information (**clinical data**), and **Electronic Protected Health Information** is defined as PHI stored on or transmitted via our computers and networks, including CDs, PDAs, tapes, and clinical equipment. An EPHI asset is a collection, application, or database of EPHI that is used for specific purposes in care delivery, or for research or education. Owner of an asset is the principal who has required and likely funded the asset to exist for care, research or education purposes, and is responsible for overall use of the information. Custodians of an asset are responsible for day-to-day operations and maintenance of hardware and software used for the asset. Institutional applications may have ownership determined by a committee of institutional stakeholders; all other assets usually have individual owners. An Information Technology person or a system administrator cannot usually be the owner of an EPHI asset.

To demonstrate compliance with the policies (specifically for EPHI assets as required by the HIPAA regulations), the owners must complete a security risk analysis for their asset. This document represents documentation for Tier A assets as defined in Information Security Management Process (EPHI1) policy. Specifically,

Tier A assets are defined as an information system or data collection (database, files, etc.) with

1. More than 20 users with or without EPHI; or
2. More than 10 devices with EPHI (servers and workstations that store EPHI data including medical devices but not workstations used only to access EPHI using an application).

In addition to completing the documents required in this list, the owners must complete the “*Information Security Risk Analysis Questionnaire for Tier A Assets*”. Owners of Tier B assets should fill out the “*Information Security Risk Questionnaire and Documentation (Limited Access)*”. For any additional information, please contact security@cpmc.columbia.edu, or the Information Security Officer.

DOC 1. ACCESS AUTHORIZATION GRID/RULES

Purpose: *Who can make a request for an account and How? What access may be given? Who validates the request? Who executes to create the account?*

Responsible: Owner and user groups

Document Cycle: Once before production, once after every major change/upgrade, annual review, and as necessary to keep current documentation

Consideration: User titles, Application/asset security levels, Application functions/modules, User work locations, IP addresses, Custodians functions, Account creation workflow, Account request form.

Questionnaire sections: (Qn_V4.0) Sections 8, 14, 15, 19, 20

Policies: EPHI1, EPHI2

1. Application/asset details (Name, Site, Owner Info)
2. Date
3. A list of **Department or Functional area**
4. For each of these, identify **who can make a request** for an account for a user (**creation, change of privileges, termination**):
 - a. (By title) Director and above.
 - b. (By name) Individual Names, and title, phone, email
5. A list of **User Roles (include Custodians if they have access to the application)**
6. For each of these, identify the **Permissible Access (es)** to the asset in a grid format
7. If required, additionally specify **Explicit Rules** that do not fit the grid format
8. Identify **Groups or individuals** who will *receive* the request
9. Identify **Groups or individuals** who will *validate* the request
10. Identify **Groups or individuals** who will *execute* the request (*eg.*, helpdesk may receive and execute, but an owner's representative validates/determines the actual access level)
11. Specify **account creation/change of privilege/termination workflow** to complete the task, including the **format of the request form (individual/list of users)**, and **methods of delivery (paper/email/fax/web forms)**
12. Specify **retention method** of the requests

DOC 2. CUSTODIAN AND VENDOR (NON-END-USER) ACCESS

Purpose: *Who are the custodians of the various sub-systems of the application/asset? What kind of access do they have towards the asset? What role does the vendor play, if any? How is access given to a vendor, if necessary?*

Responsible: Owner and custodians

Document Cycle: Once before production, once after every major change/upgrade, annual review, and as necessary to keep current documentation

Consideration: Ensure all individuals, who are non-users of the application/asset but have access to (the sub-systems of) the application/asset, are accounted for in this document.

Questionnaire sections: (Qn_V4.0) Sections 2, 8, 14, 15, 16, 22, 32

Policies: EPHI1, EPHI2

1. Application/asset details (Name, Site, Owner Info)
2. Date
3. A list of **sub-systems within the application (servers, dedicated medical or other devices, operating systems, databases, web servers, etc., and the application itself)**
4. For each of these:
 - a. Identify **Group or individual information as the Custodian** of the sub-system
 - b. Identify whether the Custodian is a **Vendor or not**
 - c. Express **the kind of access** Custodians have towards the sub-system
 - d. Identify **non-Custodians** who have access to the sub-system
 - e. Express **the kind of access** non-Custodians have towards the sub-system, and **why**
 - f. Identify **the type of training the custodian has received towards the security of the sub-system**
5. If a vendor has to be provided access to the system for a specific purpose, specify a **Procedure for provisioning of an account, logging activities, and deactivation of the account.**
6. If a vendor or a non-employee has been provided access to the system for a specific purpose, **attach a copy of the Business Associate agreement.**
7. List **various communication methods** with which the application/sub-systems are **maintained remotely** (eg., ssh, web-based, PC Anywhere, Timbuktu, VNC, Remote terminal, etc.)
8. For each of this methods:
 - a. Identify if access is over **Internet, VPN over Internet, Modems, other**
 - b. Identify **Custodian group or Individuals**
 - c. Explain **the purpose**, identifying sub-systems and functions as appropriate
 - d. Explain how the **access is limited to only the intended** group or individuals
 - e. Explain **authentication and audit logging** of actions of the group or individuals
 - f. Explain if and **what actions are necessary when an individual is no longer in the maintenance role**

DOC 3. GENERIC USERID MANAGEMENT

Purpose: *What generic (non-human) accounts exist for the Application/asset, why, and how they are managed?*

Responsible: Owner and custodians

Document Cycle: Once before production, once after every major change/upgrade, annual review, and as necessary to keep current documentation

Consideration: Generic accounts exist for (1) Execution of programs and applications, and data ownership within a system; (2) To exchange data from one system to another; (3) To provide temporary access in a special situation; (4) Extremely limited access for business reasons. Also consider the necessity to change password when a custodian is terminated. Consider how passwords of temporary accounts must be managed so that they are not usable outside their intended function.

Questionnaire sections: (Qn_V4.0) Sections 8, 14

Policies: EPHI1, EPHI2, EPHI4

9. Application/asset details (Name, Site, Owner Info)
10. Date
11. A list of **Generic accounts**
12. For each of these, identify the following:
 - a. **Date** the account is created
 - b. **Group or individual information who is Custodian** for the account.
 - c. Detailed explanation of **the purpose and use** of the account
 - d. **Procedure on when and how the password will be modified** for this account, and associated **tasks that ensure no downtime** for the asset
13. If an account is used for data transfer, identify the following:
 - a. List **the types of data** being transferred
 - b. Identify **Partner Systems/applications/assets** and **Custodians (Groups)**
 - c. **Explain how the privileges of this account are limited** to its intended function, and how **its password is protected** in a scripting environment.
14. If an account is used for temporary access, identify the following:
 - a. Explain **how a temporary account will be assigned** to an individual or a task.
 - b. Explain how **assignment of the account to an individual or a task will be logged**, and **by whom**.
 - c. Explain when and how the **account will revert back to its unassigned form**, and how will **it be logged**.

DOC 4. PORTS, SERVICES, FILES PROTECTION

Purpose: *What are the minimum necessary ports and services required for the application/asset (include operating system, databases, web and other services, as well as the application itself)? What is the extent of access to these ports?*

Responsible: Custodians, and owner

Document Cycle: Once before production, once after every major change/upgrade, annual review, and as necessary to keep current documentation

Consideration: Significant risks result from ports and services (demons in Unix) that are not essential to the application/asset, and hence must be consciously shut down.

Consider use of tools such as lsof (Unix), fport (Windows), vulnerability scans (all), process and service lists (all). Consider application and operating system maintenance functions, remote access, data transfer, etc. Encryption is preferred for all communication.

Questionnaire sections: (Qn_V4.0) Sections 12, 13

Policies: EPHI3

1. Application/asset details (Name, Site, Owner Info)
2. Date
3. A list of **open ports when the application is in operation**
4. For each of these ports, identify:
 - a. **How much open?** (Specific list of IP, specific subnets, all of Institution and affiliated subnets, Internet)
 - b. Is the **communication encrypted?** (yes or no)
 - c. Explain in detail the **purpose and use** of the open port
5. If a port is open to the Internet:
 - a. Explain **why it is open to the Internet**
 - b. Explain **why access over VPN is not sufficient or adequate** for the functions provided through the port for this asset
6. A list of **services/demons when the application is loaded and active but is not in use**
7. For each of these services/demons:
 - a. **Classify these services by identifying Subsystems** they are part of. Example would be Windows XP operating system, Oracle database, Apache WebServer, Application AppPrint, etc.
 - b. Affirm that **these services have been investigated, understood and are necessary** for the application
8. A list of **files/directory sub-trees/filesets essential to the application/asset that are excessively permitted read/write/delete/other privileges** to groups or individuals other than the custodians of the sub-system
9. For each of these files/directories/filesets:
 - a. **Classify these files/directories/filesets by identifying Subsystems** they are part of
 - b. Explain in details the **reason for excessive permission**

DOC 5. SECURITY METRICS

Purpose: *What periodic self-audit measures are deployed to confirm compliance with security rules?*

Responsible: Custodians and owner

Document Cycle: As identified

Consideration: Number of end users of the application, sample surveys.

Questionnaire sections: (Qn_V4.0) Sections 17, 18, 19, 20, 23, 24, 25, 26

Policies: EPHI3, EPHI4

1. Application/asset details (Name, Site, Owner Info)
2. Date
3. For 20% of users of the application/asset (min 5, max 20):
 - a. Investigate and report number of accounts where the user was granted **excessive privilege with missing documented approval** for the same (*Frequency:* Annually or more frequent)
 - b. Investigate and report number of accounts that **had to be terminated and were not captured by the normal termination process** (*Frequency:* Annually or more frequent)
4. Investigate and report number of **consecutive failed logins** with no intervening successful login) counting at least 5 within a 5-minute time period (*Frequency:* Monthly or more frequent)
5. For each sub-system:
 - a. Report **non-application of security patches** (*Frequency:* Quarterly)
 - b. Report number of **easily guessable passwords** (*Frequency:* Quarterly)
 - c. Report **failed or significant security events** as appropriate for the sub-system (*Frequency:* Quarterly)
6. For each **Hardware server or significant device** that comprises the application/asset
 - a. Report **Vulnerability Scan** report (*Frequency:* Before production, once after every upgrade, annually)
 - b. Report **Security Incidents** for Virus infection, compromise, denial-of-service, etc. (*Frequency:* As applicable)
7. Report any **Security Incident** associated with adverse effects to the functions of the sub-system/application/asset and the data contained therein. (*Frequency:* As applicable)
8. Address anomalies as detected, and record findings and mitigation steps, as appropriate

DOC 6. CUMC ASSET MAINTAINED IN NON-CUMC/OUTSOURCED ENVIRONMENT

Purpose: *What rules are applicable on assets that are managed in a shared NYP-University environment, or are managed in a shared NYP-Sponsored Hospital/Institution responsibility, or are managed in an outsourced environment.*

Responsible: Custodians and owner

Document Cycle: Once before production, once after every major change/upgrade, annual review, and as necessary to keep current documentation

Consideration: Complexities of joint ownerships and custodianships, whether a partner is HIPAA covered or not.

Questionnaire sections: (Qn_V3.0) Sections 21, 31

1. Application/asset details (Name, Site, Owner Info)
2. Date
3. **Fill all documentation requirements** specified in this set of documents to the degree possible and appropriate.
4. For all assets (including non-application such as network, workstations, servers, databases, etc.), if there are any components within documentation that can not be adequately addressed, communicate and discuss with corresponding asset custodian in CUBHIS for CUMC standards and with the Information Security Officer to determine completeness of documentation. **Document the decision process and the final documentation decision.**

DOC 7. PHYSICAL SECURITY, MEDIA SECURITY, MEDIA DISPOSAL

Purpose: *What physical security protection mechanisms are in effect for the application/asset?*

Responsible: Custodians and owner

Document Cycle: Once before production, once after every major change/upgrade, annual review, and as necessary to keep current documentation

Consideration: Number of physical devices that hold EPHI, and physical and environmental security controls.

Questionnaire sections: (Qn_V4.0) Sections 27, 28, 29

Policies: EPHI7, EPHI8

1. Application/asset details (Name, Site, Owner Info)
2. Date (mm/dd/yy)
3. Provide
 - a. **Number of servers, workstations, biomedical devices, and mobile devices that hold/contain EPHI in a non-transient way in day-to-day operation.** Do not include workstations that are only used to access the EPHI to show it to the users.
 - b. **Estimated number of devices that may be used to access EPHI,** including all workstations that access EPHI to show it to the users (<100, 100-1000, >1000)
4. Identify and explain the management of
 - a. **Physical access** to servers, workstations and devices holding/containing EPHI. Discuss physical security controls such as door locks, computer locks, card access, etc. Alternatively refer to an existing Data Center procedures and operations document if applicable.
 - b. **Environmental conditions** of the location where these devices are placed (Humidity, Temperature, Dust, etc.) Alternatively refer to a Data Center procedures and operations document if applicable.
 - c. Types of **passive media** used for backup (tapes, disks), and its **physical protection**. Alternatively refer to a common Backup procedure document if applicable.
 - d. **Disposal of devices and media** when they are no longer required. Alternatively refer to an existing Data Center procedures and operations document if applicable.

DOC 8. EMERGENCY ACCESS, DR/BACKUP/CONTINGENCY, SECURITY DURING EMERGENCY

Purpose: *What “availability” mechanisms are in effect for the application/asset?*

Responsible: Custodians and owner

Document Cycle: Once before production, once after every major change/upgrade, annual review, and as necessary to keep current documentation

Consideration: Communication and continuity of critical operations in case of short or long failures, short and long-term failure recovery methods.

Questionnaire sections: (Qn_V4.0) Sections 33, 34, 35, 36

Policies: EPHI2, EPHI9

1. Application/asset details (Name, Site, Owner Info)
2. Date (mm/dd/yy)
3. **Is the application/asset used for or has impact on ongoing patient care?** (yes/no)
4. If yes, provide information about the following
 - a. Provide a **list of communication methods and operational list of people to contact** when the application is unavailable.
 - b. Describe **backup methods** in place to address short-term unavailability of data and the system. Alternatively refer to a common Backup procedure document if applicable.
 - c. Describe **end-user** processes to address short-term unavailability of data and the system.
 - d. Describe **disaster recovery methods** in place to address long-term unavailability of data and the system. Alternatively refer to a common Disaster Recovery procedure document if applicable.
 - e. Describe **end-user processes to address long-term unavailability** of data and the system.

Doc 9.

Purpose: *What are the sources of EPHI data for this application? Where is EPHI data sent from this application? Are appropriate security controls in place for exchange of EPHI data?*

Responsible: Owner and custodian

Document Cycle: Once before production, once after every new exchange is put in place, annual review, and as necessary to keep current documentation

Consideration: Business Associate agreements with non-HIPAA covered entities, encryption of data transfer over public networks.

Questionnaire sections: (Qn_V4.0) Sections 22, 33

Policies: EPHI2

1. Application/asset details (Name, Site, Owner Info)
2. Date (mm/dd/yy)
3. For each EPHI data flow received from or sent to another application/asset, identify the following (do not use E-gate or other intermediary interface engines as a partner application; instead find all the final destination partner applications, and provide information. If E-gate is involved, add "via E-gate" in Direction
 - a. **Name/description of EPHI data flow**
 - b. **Direction** (ReceivedFrom/SendTo)
 - c. **Name/Description of Partner application/asset**
 - d. **Owner/Contact information** of the Partner application/asset
 - e. Is Partner application/asset **an internal CUMC/NYP application/asset or an external** one? If external, is the partner **a HIPAA Covered Entity (CE)?** (Internal/HIPAA CE/not HIPAA CE)
 - f. Is there **a Business Agreement** that is required for an external partner which is not HIPAA Covered Entity (yes/no/not applicable)
 - g. Does data flow **traverse over the Internet or other public networks**, and if so, is the flow transmission **encrypted?** (No Internet/Internet and encrypted/Internet and not encrypted)
 - h. Is the data flow associated **with clinical research?** And if so, provide the **IRB institution and IRB number** of an active research protocol. (yes/no)