Columbia University Irving Medical Center Information Security Procedures

I. OVERVIEW

A. Background

Columbia University ("Columbia" or the "University") is a HIPAA Covered Entity. For purposes of HIPAA compliance, it has organized as a hybrid entity and designated a single health care component pursuant to the Health Care Component Designation adopted and approved by the Trustees of the University on June 7, 2003, as may be amended from time to time. As a result, only the health care component is subject to HIPAA requirements. The health care component is comprised of the colleges, schools and departments that perform covered health care provider functions and other departments to the extent that they perform services in support of those functions.   For purposes of convenience the health care component is known as Columbia University Medical Center ("CUMC") and hereafter, CUMC shall be used to refer to the health care component.

B. Goal

The purpose of the CUMC Information Security Procedures (the "Procedures") is to document the detailed procedures for CUMC's implementation of the terms of the Columbia University Information Security Policies (the "Information Security Policies"), with respect to EPHI, in particular, the following Information Security Policies:

- Information Security Charter
- Information Resource Access Control and Log Management Policy
- Registration and Protection of Systems Policy
- Registration and Protection of Endpoints Policy
- Sanitization and Disposal of Information Resources Policy
- Business Continuity and Disaster Recovery Policy

The complete list of Information Security Policies can be found in the University's Administrative Policy Library under Computing and Technology Policies. Terms used, but not defined, in these Procedures are defined in Annex A hereto or the Information Security Charter (the "Charter").

These Procedures apply to the entire CUMC Workforce.   For purposes of these Procedures, the term "Workforce" includes employees, volunteers, trainees, students and other persons whose conduct, in the performance of work or study in CUMC, is under the direct control of CUMC, whether or not they are paid by CUMC.

To the extent questions arise from these Procedures relating to detailed technological standards, please refer to the University's Computing and Technology Policies or contact the Office of the Chief Information Officer at CUMC.

C. Responsibility

Responsible Official: Chief Information Officer, Columbia University Medical Center

Responsible Office: Columbia University Medical Center Information Technology

Effective Date: 11/15/2014

II. Endpoint Procedures

The procedures described in this section support the Registration and Protection of Endpoints Policy. Specific work instructions for implementing these procedures are the responsibility of the Certified IT Groups. Note that additional procedures for Medical Devices or other specialized equipment may be required.

A. Managed Endpoints

All Endpoints purchased, or subsidized, by the University and used by Workforce members will be explicitly managed by a Certified IT Group. To be explicitly managed, the Endpoint (a "Managed Endpoint") must meet the following criteria:

- All Users in the applicable business unit, and their associated Endpoints, are inventoried and inventory data are collected by the Users' Certified IT Group. Inventory data are integrated with CUMC IT's ServiceNow Configuration Management Database.
- All Managed Endpoints are required to utilize full disk encryption. All Windows endpoints must leverage, along with hardware-based TPM chips, monitoring of their encryption status by the central CUMC IT Encryption Monitoring System, as should any other system that can support this configuration. For any non-Windows system which cannot support this configuration the Certified IT Group must monitor the endpoint's encryption status and keep it current in the CUMC Asset Management System.
- In the event a user's system cannot support encryption for some reason, the user may ask for an exception by following the subsequent process:
    - A. Users will validate that no EPHI, or other Sensitive Data, are stored or accessed on the Endpoint. For circumstances where EPHI does exist on the Endpoint, but the Endpoint cannot be encrypted, the following conditions must be met:
        - i. The Endpoint is physically locked to a surface to prevent theft.
        - ii. The User submits a *Request for Encryption Exception* within the CUMC IT ServiceNow ticketing system that includes a statement of why the Endpoint cannot be encrypted and, if applicable, any plans to upgrade the Endpoint to a model that supports encryption.
    - B. Users will submit a *Request for Encryption Exception* within the CUMC IT ServiceNow ticketing system. The request will contain the following elements:
        - i. Hostname of the Endpoint;
        - ii. Type of Data accessed or stored on the Endpoint;
        - iii. The User's UNI or CWID;
        - iv. The User's supervisor;
        - v. The User's department or equivalent; and
        - vi. The User's IT Group; and,
        - vii. An explanation of why encryption cannot be supported.

C. The exception request will be reviewed by the Information Security Office and, if appropriate, routed to the User's supervisor for approval.

D. Upon approval, the request will be routed to the User's Certified IT Group, which will remove the encryption, if enabled, and add the Endpoint to a list of excepted Endpoints.

- All managed endpoints are required to have basic security software installed including, but not limited to:

  A. Anti-virus/malware (CUMC SEP recommended), and

  B. CrowdStrike Endpoint Detection and Response (EDR) agent managed by CUMC ISO
- If possible, software is enabled to permit remote wiping capabilities of the Endpoint should it be lost or stolen.
- The Endpoint is joined to a Certified IT Group's Active Directory domain, where feasible.

  A. For Endpoints that cannot be managed by an Active Directory domain, the Certified IT Group will ensure that the Endpoint has met the minimum configuration standards.
- The Endpoint is provisioned with a local IP address (10.x.x.x).

  A. Public IP addresses are only permissible by explicit authorization of the CUMC Information Security Office through the use of a *Request for Public IP Address* form.
- The Endpoint is configured to use the CUMC Proxy Server for web-based threat protection.
- The Endpoint receives timely operating System and third party application patches from the Certified IT Group.
- The Endpoint is configured to prevent the use of unencrypted and unauthorized Removable Media if supported by the operating system or management software.
- The Endpoint is configured to lock after 30 minutes of inactivity.

When a Workforce member changes functions or is no longer associated with the University, all Managed Endpoints used by the Workforce member must be returned to his/her supervisor. At this time, the endpoint inventory must be updated to reflect the current status of the endpoint, either decommissioning/disposal, reassignment with new owner noted, etc.

B. Personal Endpoints

The use of personally owned Endpoints (e.g. "Bring Your Own Device", aka BYOD) to access secured CUMC assets by a Workforce member is permissible only if the following conditions are met:

- The User agrees to grant the Certified IT Group administrative rights to and management of his/her Endpoint while the Endpoint is being used for CUMC purposes as long as the device meets the specifications for FDE and EDR; and
- The User agrees to allow the Endpoint to be monitored by his/her Certified IT Group.

1. Request for Personal Endpoint Authorization

A department and associated CITG may, or may not, choose to allow members of their department to use personally owned endpoints. If they do, the following procedure applies:

1. The User submits a *Request for Personal Endpoint Usage* form in the CUMC IT ServiceNow system.
2. The User's supervisor is notified via email of the access request.
3. The User's supervisor reviews and approves or rejects the access request. If rejected, the User is notified via email.
4. If approved, the User's HIPAA Privacy and Security training status is evaluated and if all trainings are current, the approval is forwarded to the User's Certified IT Group via email for their approval. If the trainings are not current, the User and the User's supervisor are notified and the request is rejected.
5. If approved, the User's Certified IT Group configures the Endpoint so that it may be fully managed and enters it into the CUMC Asset Management Database.
6. The Endpoint is returned to the User for use.

All requests will be documented, stored and maintained in the CUMC IT ServiceNow system with an appropriate retention period.

When a Workforce member is no longer associated with the University, the workforce member's department – via their Certified IT Group – is responsible for ensuring that any CUMC Data on his/her personally owned Endpoints is sanitized in accordance with the Sanitization or Disposal Procedures.

C. Data Backup

If any Endpoint is the primary repository of EPHI, the User of the Endpoint must comply with Section III(C) of the Business Continuity and Disaster Recovery Policy relating to Data Backup Plans.

D. Approved Usages of Removable Media

Workforce members may only use Removable Media that meet all of the following security criteria:

- Encryptable Data to 256-bit AES Cipher-Block & FIPS Validations: 140-2
- USB 2.0 and higher (for USB connected media)
- Supports complex passwords on the media
- The drive locks down and reformats after a maximum of ten intrusion attempts
- Ability to disable auto run

CUMC IT maintains a list of approved Removable Media, and Certified IT Groups will only permit Removable Media that meet the above requirements to connect to Managed Endpoints.

At no time shall unencrypted Removable Media be used. Exceptions will be permitted on a case-by-case basis, if approved by a User's supervisor as well as his/her certified IT Group. This exception can be requested through the *Request for Encryption Exception* form, as described in Section A above.

When a Workforce member changes functions or is no longer affiliated with CUMC, all Removable Media must be returned the User's supervisor. Media may then be redeployed, in accordance with the Sanitization or Disposal of Internal Media and Removable Media procedure.

E. Third-Party Software Applications

All third-party software applications that do not process or store information directly on the endpoint must undergo an IT software review prior to use. This includes any applications, plug-ins, modules, or integrations, many of which may use external Cloud storage.

In accordance with the University's policies for External Hosting and Registration And Protection Of Endpoints, users must contact their Certified IT Group well in advance to initiate an application review of third-party software. Each department that owns or uses a third-party software is responsible for ensuring that the necessary review and approval is granted before deployment.

A review performed on third-party software may require different assessment workflows. Application assessments are evaluated based on criticality and sensitivity as determined by the software capabilities and interaction with institutional data as categorized under the University's Data Classification policy.

III. Sanitization or Disposal Procedures

The procedures described in this section support the Sanitization and Disposal of Information Resources Policy. Sanitization and disposal tasks will be conducted by Certified IT Groups. Work instructions for these procedures will be documented and maintained by Certified IT Groups. A template of these work instructions will be developed by the CUMC Information Security Office and provided to Certified IT Groups to be completed for their specific implementations.

A. Basic Sanitization/Disposal Procedure

When an Endpoint or Removable Media will be retired, a specific set of procedures must be followed, based on the circumstances of the situation. All requests will follow the following basic procedure:

1. A *Request for Sanitization or Disposal* form will be filled out by the User of the Endpoint in the CUMC IT ServiceNow system.
2. The *Request for Sanitization or Disposal* will indicate one of the following requests:
    a. Disposal of the Endpoint;
    b. Disposal of the internal media of the Endpoint;
    c. Sanitization of the internal media of the Endpoint so it may be repurposed; or
    d. Sanitization of the Removable Media.
3. The appropriate Certified IT Group will be notified via email of the User's request.
4. The appropriate IT Custodian within the Certified IT Group will carry out the request and ensure that all documentation in the CUMC IT ServiceNow system is complete. The documentation will contain, at a minimum:
    a. Make and Model of Endpoint or Removable Media;
    b. Serial Number, if applicable;
    c. MAC address (network interface hardware address), if applicable;
    d. Dates of disposal/sanitization; and
    e. Method used for sanitization or disposal.
5. The IT Custodian will update the Certified IT Group's inventory to reflect that the Endpoint or Removable Media has been decommissioned.

All requests will be documented, stored and maintained in the CUMC IT ServiceNow system for a period of 6 years.

1. Disposal of Managed Endpoints

If a User asks for a Managed Endpoint to be disposed of, the following procedures will be followed in addition to the Basic Sanitization/Disposal Procedure described above:

1. The User will indicate on the *Request for Sanitization or Disposal* form "Dispose of the Endpoint".
2. The relevant additional identifiers of the Endpoint will be captured, including:

   a. Hostname;
   b. UNI/CWID of the User; and
   c. Endpoint location.
3. The Endpoint will be collected from the User by the User's Certified IT Group and stored in a physically secured location, with an access badge reader and video surveillance, prior to disposal.
4. The internal media of the Endpoint will be removed, and if not immediately disposed of, will be labeled to indicate the Endpoint from which the media was removed.
5. The internal media will be destroyed and rendered inoperable through methods described in the Sanitization and Disposal of Information Resources Policy. This process will be documented by the Certified IT Group in the CUMC IT ServiceNow system.
6. A green Device Disposal Tag will be affixed to the Endpoint.
7. The Endpoint and/or destroyed media will be given to Facilities Management, which will work with the Department of Environmental Health and Safety to dispose of the Endpoint and media in an environmentally conscious manner.

2. Sanitization or Disposal of Personally Owned Endpoints

When a User is no longer affiliated with CUMC, all CUMC Data must be sanitized or destroyed. Managers of departments or business units are required to ensure that personally owned Endpoints are properly sanitized or disposed of before the User leaves CUMC. The following procedure will be followed:

1. The User's supervisor will indicate on the *Request for Sanitization or Disposal* form either:
   a. "Sanitize Data from Personally Owned Endpoint" or
   b. "Dispose of Personally Owned Endpoint".
2. The relevant additional identifiers of the Endpoint will be captured, including:
   a. Hostname;
   b. UNI/CWID of User; and
   c. Endpoint location.
3. An IT Custodian of a Certified IT Group will conduct the secure deletion of CUMC Data from the personally owned Endpoint, or will follow the Disposal of Managed Endpoints procedure described in Section A.1 above if the device will be disposed of.

B. Sanitization or Disposal of Internal Media or Removable Media

If any internal media or Removable Media in an Endpoint contain EPHI, the following special procedures must be followed when the internal media or Removable Media are to be disposed of, or re-provisioned for non-EPHI use.

1. Procedure

If requested by the department or business unit, the internal media or Removable Media of an Endpoint may be disposed of rather than the entire Endpoint itself. In this circumstance, the Disposal of Managed Endpoints Procedure described in Section A.1 above will be followed, with the following changes:

1. The User will indicate on the *Request for Sanitization and Disposal* form the specific request. The options are:
    a. Disposal of internal media;
    b. Sanitization of internal media;
    c. Disposal of Removable Media; or
    d. Sanitization of Removable Media.
2. The request will be forwarded to the User's Certified IT Group by email.
3. The Certified IT Group will (a) tag any media to be disposed of, or (b) secure wipe any media selected to be sanitized. In either case, the Certified IT Group will process the request based on the methods described in the Sanitization and Disposal of Information Resources Policy.

All requests will be documented, stored and maintained in the CUMC IT ServiceNow system for a period of 6 years.

IV. IT Group Certification

The procedures described in this section support the Information Security Charter, specifically as it relates to IT Groups. The following principles and procedures apply to all IT Groups:

- All Users within CUMC are required to be supported by a Certified IT Group.
- IT Custodians must be members of an IT Group.
- Each IT Group will have an IT Group Manager who is responsible for managing the IT Group.
- All IT Group Managers will have a dotted line relationship to the CUMC Chief Information Officer.
- IT Groups will, to the best of their ability, implement enterprise policies, procedures and standards, defined by CUMC IT, in a consistent and uniform manner.
- The CUMC Information Security Office will be responsible for analyzing and certifying that the IT Group is operating in a capacity that is consistent with University Policies and Procedures, as well as operating within an acceptable level of risk, as defined by CUMC Executive Managers.

A. Registration of IT Groups

All IT Groups must be registered with the CUMC Information Security Office by the Manager of the IT Group by submitting an *IT Group Registration* request email that includes the following information:

1. The name of the IT Group;
2. The constituents the IT Group serves (departments, divisions and/or business units);
3. The name of the Manager of the IT Group;
4. The IT Group's Executive Manager; and
5. A complete list of all IT Custodians employed by the IT Group. This list will contain the following elements for each individual IT Custodian:
    a. UNI
    b. The department or business unit the IT Custodian is employed by (preferably with the Department ARC ID)
    c. The IT function or service provided (e.g., desktop management, server administration, application administration, developer)
    d. The name of the IT Custodian's supervisor

B. Certification of IT Groups

IT Groups must be certified by the CUMC Information Security Office in accordance with standards developed by the CUMC Information Security Office. The CUMC Information Security Office will be responsible for setting the prerequisites for each level of certification and each IT Group will be risk assessed by the CUMC Information Security Office to determine which level of certification is needed and to ensure that the applicable requirements have been met.

IT Groups will have their operations re-evaluated on a periodic basis, based upon risk.

C. Certification

1. General Requirements

All Certified IT Groups will be risk assessed and certified to be compliant with the following:

- The IT Group has a standard method of collecting and integrating inventory Data with the CUMC IT ServiceNow Configuration Management Database;
- Standard services for Users have been deployed in a secure manner, including desktop management, server management and lab management;
- The IT Group has a process for informing the CUMC Information Security Office of any reportable security events or incidents; and
- All IT Custodians in the IT Group have received security training commensurate with their Workforce function.

2. For IT Groups with Certified Systems

In addition to the General Requirements listed above, all Certified IT Groups who manage Certified Systems are to be compliant with the following:

- The IT Group has provided evidence of compliance with the Access Control Policy and Procedures;
- The IT Group has provided evidence that all Managed Endpoints are in compliance with the Endpoint Policy and Procedure;
- The IT Group has established practices for monitoring EPHI in Systems it manages;
- The IT Group participates in the Change Management Process for Certified Systems; and
- The IT Group has agreed to provide monthly status reports to the CUMC Information Security Office on key performance indicators and metrics.

V. System Registration and Protection Procedures

The procedures described in this section support the Registration and Protection of Systems Policy. Work instructions for these procedures will be documented and maintained by Certified IT Groups. Note that additional procedures for Medical Devices or other specialized equipment may be required.

A. System Operation

All Systems, and their underlying components (such as Servers), that process, transmit and/or store EPHI must be explicitly managed by a Certified IT Group. To be explicitly managed, the System must meet the following criteria, in addition to the criteria referenced in the Registration and Protection of Systems Policy:

- The System has been scheduled for regular vulnerability scanning by the CUMC Information Security Office,
- The System has been scheduled for daily DLP scanning by the CUMC Information Security Office.
- The System is provisioned to use a local IP address (10.x.x.x).
    A. Public IP addresses are permissible only by explicit authorization by the CUMC Information Security Office through a *Request for Public IP Address* form.
- The underlying Server, if possible, will be joined to an Active Directory domain managed by the Certified IT Group
    A. For Servers that cannot be managed by an Active Directory domain, the Certified IT Group will ensure that the Server has met the minimum configuration standards.
- Any environmental or operational changes made to the System, or its underlying components, will be first authorized through the Change Management Process.
- A set of standards will be developed and maintained by the Certified IT Group to ensure a consistent configuration and management methodology that aligns with the University Computing and Technology Policies.
    A. Reference should be made to the UNIX and Web servers "Standard Operating Environment and Security Best Practices" documents maintained by CUIT.

B. *System Registration Procedures*

All Systems within CUMC must be registered with the CUMC Information Security Office in accordance with the following procedure:

1. After determination the System will be acquired, the System Owner, or IT Custodian, will access RSAM (https://rsam.cumc.columbia.edu) and fill out the System Registration object.
    a. Work instructions for this procedure will be documented by the CUMC Information Security Office, and can be found on the RSAM System Registration Walkthrough website.
2. The business purpose and functions of the System must be clearly identified. This will include the following attributes:
    a. The number of users of the System;
    b. The number of records the System holds; and
    c. The date the System went, or will go, into production.
3. Other demographic information must be captured, including:
    a. System Owner;
    b. IT Custodian(s);
    c. Other stakeholders;
    d. Classification of Data stored or processed by the System (Sensitive, Confidential, Internal or Public);
    e. Location of the Servers' Data Center;
    f. The types of services the System provides (such as Application, Database, Email, etc;)

   g. Flow of Data (especially Sensitive Data) into and out of the System;
   h. Types, amounts and identifiable characteristics, of Data processed, transmitted and/or stored;
   i. Users of the System;
   j. Exposure of the System to the Internet; and
   k. Maximum allowable permissible downtime.
4. All servers supporting the System must be inventoried and documented. This information should be entered into RSAM, with the following attributes:
   a. IP Address;
   b. Hostname;
   c. Operating System; and
   d. Server's purpose.

C. System Risk Analysis

Systems that have been registered with the CUMC Information Security Office will be evaluated based on the risk they introduce into CUMC. This is done through a number of steps and via the following general procedures:

1. Newly registered Systems will undergo an initial "inherent risk" evaluation by the CUMC Information Security Office to determine the criticality of the System and the amount of risk it introduces into CUMC. This evaluation will take into account:
   a. The classification of Data stored or processed on the System;
   b. The number of uniquely identifiable records stored on the System;
   c. The number of Users of the System; and
   d. The exposure of the System to the Internet.
2. A Controls Based Assessment (CSA) will be provided to the System Owner, which will contain a list of controls based on the nature of the System. The System Owner is responsible for evaluating the configuration of the System against the CSA and providing the results to the CUMC Information Security Office.
3. The CUMC Information Security Office will review the results of the CSA and identify any gaps that might exist. Gaps that have been identified will be classified as vulnerabilities.
4. The CUMC Information Security Office will conduct a technical vulnerability scan against all Servers comprising the System. The results of the vulnerability scan will be added to the list of identified vulnerabilities.
5. The CUMC Information Security Office will evaluate the threats associated with any technical vulnerabilities and/or any vulnerabilities discovered during the CSA analysis. This threat to vulnerability mapping will result in an evaluation and rating of the gaps with a risk score.
6. All risks are described by three descriptive components, namely:
   a. *Issue* – the reason why the determined gap is a problem
   b. *Risk* – a statement about the risk the gap introduces to the organization and its impacts

c. *Solution* – a recommended resolution to remove or mitigate the risk

7. An overall risk score of the System will be recorded based on the highest level of any individual component risk. E.g., if a System is deemed to contain 5 risks comprised of 4 low risks and 1 high risk, then the overall risk of the System will be "High".
8. A final report will be compiled by the CUMC Information Security Office, comprised of an executive summary, detailed risk findings and technical vulnerability results, and submitted to the Executive Manager of the department or business unit. If the System contains no risks it will be given a score of "Pass" and will be immediately granted "Certified" status.

D. System Remediation

Any System that is found to have risks must undergo a formal Corrective Action Plan and the development of a Plan of Action and Milestones. The following procedures will be followed:

1. The System Owner, upon receiving the risk analysis report, will evaluate the risks discovered.
2. Within 30 days, the System Owner will respond to the risks identified and either (a) agree with the findings and submit the Corrective Action Plan for remediation of each individual risk, or (b) contest the risk finding.
    a. Should the System Owner contest the risk, the System Owner and the CUMC Information Security Office will review it. If the CUMC Information Security Office agrees with the contestation, the risk will be removed. If it does not agree, then mediation will take place. Mediation will ensure that both parties come to agreement. If necessary, the risk discussion will be escalated to Executive Management for final mediation.
3. If the System is given a Critical or High risk score, an emergency risk plan will be developed by the System Owner to execute remediation of the Critical or High risks within 7 days of report issuance. The focus of the plan is to remediate the urgent risks in a timely manner so they are not exploited.
4. After the remediation plan has been submitted to the CUMC Information Security Office and approved by Security Managers, the System Owner will have 90 days to execute the plan.
5. While the System is under remediation, System Owners will regularly report to the Security Managers the status of the remediation. In addition, Security Managers will periodically check the status of the remediation with the System Owner.

E. System Certification

Upon attestation from the System Owner that all risks have been mitigated, the CUMC Information Security Office will initiate a final check to provide the appropriate level of assurance that the risks have been properly mitigated. The following procedure will be followed:

1. Security Managers will review the System's risks and the remediation plan.

2. Security Managers will evaluate the controls implemented by the System Owner and test that the controls appropriately mitigate the risk. System Owners will be required to provide evidence of all controls implemented to mitigate the risks.
3. If the controls are deemed adequate and all risks have been mitigated to an acceptable level of tolerance, Security Managers will issue a Certification Report to the System Owner and his/her Executive Managers.
4. The System will be updated in the RSAM list of CUMC Certified Systems.
5. The System will be scheduled for re-certification at a later date, based upon the inherent risk of the System. The higher the inherent risk of the System the more frequent the risk analysis will be conducted.

F. New System Governance Process

All new Systems that will process, transmit and/or store EPHI must first be approved for use through an IT Steering Committee governance process. System Owners will submit their requests to the IT Steering Committee, which in turn will confirm that the System is filling a particular business need (clinical, research or administrative) and that the proper party to develop, implement and maintain the System has been identified. The process is as follows:

1. The System Owner, IT Custodian or User will submit a *Request for Approval to Implement New System* email to the CUMC CIO. The email will contain, at a minimum, the following information:
    a. Business need the System will fulfill;
    b. Evaluation of skills and capabilities needed to run the System;
    c. Priority of the request; and
    d. Constituents and Users who will use and/or be impacted by the System.
2. The email will be forwarded to the IT Steering Committee for review.
3. The IT Steering Committee will evaluate the request, using the following criteria:
    a. If the request has a legitimate business need that is not currently available from an existing System;
    b. If the proposed System Owner's Certified IT Group has the appropriate skills and capabilities to implement, manage and monitor the System; and
    c. If the business need is required by more than the individual department or business unit, whether the System should be hosted locally within the Certified IT Group or centrally by CUMC IT.

After all evaluations have been conducted, the IT Steering Committee will provide a final approval or rejection.

G. Data Backup

For all Systems containing EPHI, the System Owner must comply with Section III(C) of the Business Continuity and Disaster Recovery Policy relating to Data Backup Plans. For such Systems, the Data

Backup Plan should address whether a backup of EPHI is needed before any movements of the System (e.g., to a new location).

VI. Change Management Process

A. *Purpose*

CUMC evaluates all environmental and operational changes to ensure they do not adversely affect the security of its EPHI, and provides a formal and standardized methodology for responding to change. The result of this process (a) ensures security of EPHI during an environmental or operational change, (b) improves the quality of changes and (c) reduces the impact of changes on day-to-day operations.

The change management process is used to meet the following principles:

- Control over IT environment
- Communication and collaboration of production changes
- Improve the confidence in implementation of changes
- Improve the consistency of service

To that end, the following process should be followed (a) throughout all areas of CUMC where EPHI is processed, transmitted and/or stored, (b) where the Systems are used in a production capacity or (c) where the infrastructure components are used to support these production Systems.

For the purposes of this process, any System that processes, transmits and/or stores EPHI and is accessible to the general network or the Internet, must be considered to be "in production". For example, a test or development system exposed to the Internet would be considered "in production", due to its exposure.

B. *Roles and Responsibilities*

1. Change Owner

The Change Owner is responsible for overall Process Governance, including:

- Defining the overall mission of the process;
- Communicating the process mission, goals and objectives to all stakeholders;
- Resolving any cross-functional (departmental) issues;
- Reporting on the effectiveness of the process to CUMC senior leadership; and
- Initiating process improvement initiatives.

2. Change Manager

The Change Manager is responsible for day-to-day Process Management, including:

- Tracking compliance with the process;

- Escalating issues relating to the process
- Gathering and reporting on process metrics;
- Performing specific operational duties;
- Convening and chairing Change Review Board (CRB) meetings;,
- Ensuring that the Forward Schedule of Changes is kept current and made available;
- Conducting Post-Implementation Reviews for those changes for which such reviews are deemed necessary;
- Analyzing change records to determine any trends or issues and seeking correction by the relevant parties;
- Authorizing Change Process Templates (for Standard Changes);
- Being the final confirmation point for Emergency Changes;
- Submitting Unauthorized Requests for Changes (RFCs); and
- Closing RFCs.

3. Change Requester

The Change Requester is responsible for requesting the change, including providing the details regarding the change, its business justification, as well as the accuracy and completeness of the request. The Change Requester may be a User or an IT Custodian and may also be the Change Submitter.

4. Change Submitter

The Change Submitter fills out the RFC and submits it on behalf of him/herself (or a separate Requester) and has the following responsibilities

- Recording the details regarding the change, including the business justification as well as the accuracy and completeness of the request;
- Recording the change’s risk factors;
- Providing all necessary supporting documentation for the change (e.g., implementation tasks, test plans and back-out plans) and the location of the source Data; and
- Canceling the RFC.

5. Change Review Board

The Change Review Board **(CRB)** is a standing board of peers that advises, or assists, the Change Manager, retains the authority to approve or reject changes and has the following responsibilities:

- Approving RFCs;
- Preparing the Forward Schedule of Change;
- Executing Post Implementation Reviews; and
- Approving Change Process Templates.

The Members of the Change Review Board will include:

- Change Manager
- Information Security Delegate
- CUMC Deputy Chief Information Officer (CIO)
- CDIS Delegate (representing enterprise applications)
- DBMI Delegate (representing research and Data warehousing)
- CORE (representing networking)
- Rotating Delegate #1
- Rotating Delegate #2
- Rotating Delegate #3

Once every 12 months, a delegate will be selected from the Certified IT Groups to serve for a period of 12 months on the Change Review Board. The CUMC CIO, or his/her delegate, will select the delegates. Delegate start dates will be staggered by four months so that only one delegate will be changed at any given time.

6. Emergency Change Review Board

The Emergency Change Review Board (ECRB) is a subset of the CRB that may be called upon at any time to provide advice to the Change Manager when dealing with an Emergency Change.

C. Change Process

The CUMC CIO will be the change management process owner. Each Certified IT Group will participate in the central CUMC IT change management process. The process will be as follows:

- A Change Requester will determine the need for a change. The Change Requester will work with a Change Submitter (or the Change Requester can also serve as the Change Submitter) and create a RFC in the CUMC IT Service-Now system. Once complete, the RFC will be submitted to the Change Manager. The RFC will contain the following information, filled out by the Change Submitter:
    - Description of change;
    - Type of change;
    - Business justification for change;
    - Business impact if the change were to fail;
    - Requested date of change, to be later put on the Forward Schedule of Changes;
    - Back out plan;
    - Testing plan; and
    - Security risk evaluation, which will include an evaluation of the confidentiality, integrity and availability of the change. Special Standard Operating Procedures will be created to account for the different types of Systems, including those with EPHI.

- The Change Manager will review the change to ensure that all elements are complete. If complete, the status of the RFC will be changed to “Pending Approval” and will be added to the weekly CRB meeting agenda.
- The CRB will review the RFC during the weekly Change Management meeting. The CRB will review the change based upon the type of change being submitted. In general, the CRB will look at elements such as security risk evaluation, authorization, proposed schedule, implementation date, testing and back out plans. The Change Requester will receive an email notification whether the change was approved or rejected.
- If the change is approved, the Change Manager will add the RFC to the Forward Schedule of Changes.
- If the change is approved, the Change Requestor may implement the change based upon the Forward Schedule of Changes.
- If the change is successful, the Change Requester or Change Submitter will update the RFC to reflect the completion of the change. If the change was unsuccessful, the Change Requester will reverse the change in accordance with the back-out plan and will document the reversal in the RFC.
- The Change Manager will review the complete change process and evaluate whether the change should be added to the Post Implementation Review log.

1. Types of Changes

Normal: The default change state. This is a change that is submitted with sufficient lead-time (14 calendar days) and that represents a risk to the security of EPHI or the service.

Expedited: A fast-tracked normal change that meets all of the criteria for a normal change, but must be completed in less than 14 calendar days. Justification must be supplied for this type of change.

Routine: A change that has been performed reliably many times in the past and that does not pose a significant risk to services. This type of change can be pre-approved by the Change Manager and the CRB, and as such does not require specific CRB approval. However, the Change Requester using one of the predefined change request templates must still submit a RFC.

Emergency: A change that is being implemented to correct an ongoing or potential service outage. Examples include: fixing infrastructure that has failed, protecting a service from an unacceptable risk of degradation, or avoiding a regulatory compliance issue. This change must be approved by the ECRB.

Unauthorized: Changes that have been implemented outside of the approval and governance of the Change Management Process. Unauthorized changes are reviewed by the CRB during the Post Implementation Review process.

2. Specific Types of Change Procedures

In addition to the basic process described above, special circumstances exist for different types of changes requested. The Change Process described above defines a "Normal" change. The additional exceptions are indicated below.

Routine Change

- The Change Requester will select "Standard Change" on the RFC template. If there is no RFC template, this type of change cannot be selected.
- The Change Manager will evaluate the RFC. The Change Manager will ensure that the change request meets the criteria of a "Standard Change". An example of a Standard Change includes patching an operating system with security patches.
- The Change Manager will approve changes that meet the requirements. Other changes will be rejected.
- The process will continue as it would for a Normal Change.

Expedited Change

- The Change Requester will select "Expedited Change" on the RFC template due to a business need that requires completion of the change earlier than 14 days from the date the RFC was submitted.
- The Change Manager will review the business justification for the expedited change. If appropriate, the Change Manager will approve the change. If not, the Change Manager will reject the change and will so notify the Change Requester.
- Changes approved by the Change Manager will be forwarded to the CRB.
- The Change Requester will present the change to the CRB, and the reasoning for the expedited status.
- The CRB will approve or reject the change, and the process will continue as it would for a Normal Change.

Emergency Change

- The Change Requester will call the ECRB hotline, explain the circumstances and ask for verbal approval. The Change Requester will note who gave the verbal approval. If the ECRB cannot be reached, the Change Requestor will contact the Change Manager for the same approval.
- The Change Requester will indicate "Emergency" status on the RFC and provide the name of the ECRB member who gave verbal approval.
- The Change Requester, or his/her delegated IT Custodian, will implement the emergency change.

- After the change has been completed, the Change Requester will update the RFC with the following information:
  - Nature of the emergency;
  - Length of downtime;
  - Cause of the emergency;
  - Resolution;
  - Whether the resolution is permanent and if it is not, what the plans are for permanent remediation;
  - How the emergency could have been avoided.
- Emergency changes will be reviewed at the regular CRB meeting. The Change Requester must be present at the CRB Change Management meeting to explain the reason for the emergency change.
- All emergency changes will be put on the Post Implementation Review agenda to be reviewed by the Change Manager, System Owner, and any other relevant parties, at a later date.

Unauthorized Change

Upon notification or detection of an unauthorized change, the following procedure will occur:

- The Change Manager will create a RFC.
- The Change Manager will investigate why the change occurred in an unauthorized fashion, and document all relevant facts of the investigation.
- The unauthorized change will be discussed at the next CRB meeting.
- The unauthorized change will be put on the Post Implementation Review agenda to be reviewed by the CRB at a later date.
- The CRB will determine if follow-ups, or sanctions, are necessary.

D. Post Implementation Review

Post Implementation Reviews (PIRs) are “after the fact” reviews of specific changes that meet one or more of the following criteria:

- A change that created an unknown/unexpected impact to service
- A change that failed
- A change that was not properly communicated
- A change with further impact than indicated from the review process
- A change that was classified as an “Emergency” or “Unauthorized”
- A random selection of successful changes

The goal of a PIR is to determine if lessons can be learned based on specific change examples, which can help provider further service improvement.

1. PIR Procedure

All PIRs must take place within 7 business days of the change event to ensure that all parties have up to date knowledge of the change event. The following procedure will be followed:

- The Change Manager will review the change log and select the appropriate RFCs for PIR.
- The Change Manager will coordinate a detailed investigation with all parties involved and will ensure that a detailed analysis of what went wrong and lessons learned for future improvement is documented.
- The IT Custodians involved will complete a *PIR Problem* form in the CUMC IT Service-Now system, to document a detailed set of events associated with the RFC.
- The Change Manager will determine what action items will be undertaken and their deadlines

E. Metrics

The following metrics will be used for periodic assessment of the change management process.

Number of RFCs resulting in an Incident

Description	This may be the most significant indicator of the effectiveness of the process as making changes without impacting the business is what Change Management strives to do. Ideally this number would be zero.
Type	Number
Opportunity for Defect	Incorrectly entered Request For Change (RFC) where the services affected are not ident ified properly may mean that the risk has not been properly evaluated and unexpected results may occur when the change is implemented
Measurement Procedure	A count of all Incidents created during the period that were related back to a specific authorized Request For Change (RFC) or identified tasks.
Additional Details	Number of authorized Request For Change (RFC) (including associated tasks) that result ed in a reported incident.

Number of Authorized RFCs

Description	An indication of the volume of Request For Change (RFC) and tasks passing through the Change Management system.
Type	Number
Opportunity for Defect	A high volume of Request For Change (RFC) without adequate time for review may me an that changes are being authorized without being correctly reviewed
Measurement Procedure	A count of all Request For Change (RFC) authorized during the period.
Additional Details	Total number of Request For Change (RFC) flowing through the system that have been authorized during the time period.

Number of Unauthorized RFCs

Description	An indication of the volume of unauthorized changes that have not been added to the Change Management System.
Type	Number
Opportunity for Defect	This requires that the Change Manager be able to determine that an unauthorized change occurs. There is not a “known denominator”
Measurement Procedure	A count of all Request For Change (RFC) Unauthorized during the period
Additional Details	Total number of Request For Change (RFC) flowing through the system that have been Unauthorized during the time period

Ratio of Emergency RFCs

Description	Emergency changes pose a potential risk to the business, as they are introduced in an accelerated time frame. This number should be a small percentage of the overall changes
Type	Ratio
Opportunity for Defect	The Emergency classification may be used to bypass standard lead-time requirements when the change would otherwise not qualify as an emergency.
Measurement Procedure	A count of all emergency Request For Change (RFC) divided by the total number of changes for the period X 100
Additional Details	All Request For Change (RFC) classified as emergency change types as a percentage of the overall changes handled during the period

Total Number of RFCs by Change Type

Description	Presented by Period and depicted over time will indicate a trend that can be observed and acted upon.
Type	Number
Opportunity for Defect	
Measurement Procedure	Simply a count of all Request For Change (RFC) created during the period
Additional Details	

Change Tasks by Group

Description	Number of Change Tasks Implemented by group over a period of Time
Type	Number
Opportunity for Defect	
Measurement Procedure	Simply a count of all Request For Change (RFC) created during the period, summarize over time and trend.
Additional Details	

VII. ANNEX A: DEFINITIONS

Columbia or the **University:** Columbia University

Columbia University Medical Center: the health care component of the University that is comprised of the colleges, schools and departments that perform covered health care provider functions and other departments to the extent that they perform services in support of those functions, as specified in the Health Care Component Designation adopted and approved by the Trustees of the University on June 7, 2003, as may be amended from time to time.

Confidential Data: any information that is contractually protected as confidential information and any other information that is considered by the University appropriate for confidential treatment. See the Columbia University Data Classification Policy [http://policylibrary.columbia.edu/data-classification-policy] for examples of Confidential Data**.**

Covered Entity: as defined in the HIPAA Privacy Rule (45 CFR 160.103).

CUMC: Columbia University Medical Center

CUMC Information Security Office: Columbia University Medical Center Information Security Office.

CUMC IT: Columbia University Medical Center Information Technology.

Data: all items of information that are created, used, stored or transmitted by the CUMC community for the purpose of carrying out the institutional mission of teaching, research and clinical care and all data used in the execution of CUMC's required business functions including but not limited to EPHI.

Data Owners: CUMC officials, including Directors, Officers of Instruction and Officers of Research, who are responsible for determining Data classifications, working with the CUMC Information Security Office in performing risk assessments and developing the appropriate procedures to implement the Information Security Policies in their respective areas of responsibility.

Endpoint: any desktop or laptop computer (i.e., Windows, Mac, Linux/Unix), Mobile Device or other portable device used to connect to the University wireless or wired Network, access Columbia email from any local or remote location or access any institutional (University, NewYork-Presbyterian Hospital, departmental or individual) System either owned by the University or by an individual and used for CUMC purposes.

EPHI: Electronic Protected Health Information.

FERPA: the Family Educational Rights and Privacy Act

HIPAA: the Health Insurance Portability and Accountability Act

HITECH: the Health Information Technology for Economic and Clinical Health Act and its implementing regulations as amended and supplemented by the HITECH Act and its implementing regulations, as each is amended from time to time.

Information Resource: (a) all Data regardless of the storage medium (e.g., paper, fiche, electronic tape, cartridge, disk, CD, DVD, external drive, copier hard drive, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.); (b) the computing hardware and software Systems that process, transmit and store Data; and (c) the Networks that transport Data.

Information Security Office: the CUMC Information Security Office or the Columbia University Information Security Office.

IT Custodians: CUMC personnel who are responsible for providing a secure infrastructure in support of Data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges as authorized by Data Owners or System Owners and implementing and administering controls over Data in their respective areas of responsibility.

IT Group: A group of IT personnel who, as full-time employees of the Medical Center or a member of the CUMC OHCA, are responsible for providing a secure infrastructure in support of data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges as authorized by Data Owners or System Owners and implementing and administering controls over data in their respective areas of responsibility. For more information, refer to the Certified IT Group Program Specifications (PDF).

Mobile Device: a smart/cell phone (i.e., iPhone, Blackberry, Android, Windows phone), tablet (i.e., iPad, Nexus, Galaxy Tab and other Android based tablet) or USB/removable drive.

Network: electronic Information Resources that are implemented to permit the transport of Data between interconnected endpoints. Network components may include routers, switches, hubs, cabling, telecommunications, VPNs and wireless access points.

PCI: Payment card industry.

PCI-DSS: the PCI Data Security Standard produced by the PCI–SSC, which mandates compliance requirements for enhancing the security of payment card data.

PCI-SSC: the PCI Security Standards Council, which is an open global forum of payment brands, such as American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc, that are responsible for developing the PCI-DSS.

Protected Health Information: any information created, received, maintained, processed or transmitted by CUMC that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for health care and (a) identifies the individual or (b) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Removable Media: CDs, DVDs, USB flash drives, external hard drives, Zip disks, diskettes, tapes, smart cards, medical instrumentation devices and copiers.

Security Managers: Managers in the CUMC Information Security Office. Security Managers are responsible for the day to day management of CUMC's Information Security Program.

Sensitive Data: any information protected by federal, state and local laws and regulations and industry standards, such as HIPAA, HITECH, FERPA, the New York State Information Security Breach and Notification Act, similar state laws and PCI-DSS. See the Columbia University Data Classification Policy [http://policylibrary.columbia.edu/data-classification-policy] for examples of Sensitive Data**.**

Server: a Server is a computer that provides a service to other computers, such as processing communications, file storage, or accessing a printing facility. There are many types of Servers including web, database, application, authentication, DNS, mail, proxy, and NTP Servers.

System: A System is a multi-user application or service used for University purposes which resides on one or more computing device(s) and transmits, stores, or processes University data. Any business process and/or application running on a Server is a System. Individual Endpoints are not considered Systems, unless they are performing Server functions.

System Owners: CUMC officials, including Directors, Officers of Instruction and Officers of Research, who are responsible for determining computing needs, and applicable System hardware and software, in his/her respective areas of responsibility and ensuring the functionality of each such System.

User: a person who uses Information Resources. Users are responsible for ensuring that such Resources are used properly in compliance with the Columbia University Acceptable Usage of Information Resources Policy [http://policylibrary/columbia.edu/acceptable-usage-information-resources-policy], information is not made available to unauthorized persons and appropriate security controls are in place.

VPN: Virtual Private Network.