DEFINITIONS

"Protected Health Information" or "PHI" is any individually identifiable health information, in any form or media, whether electronic, paper, or oral. "Individually identifiable" means that the health or medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, genetic or other information that, alone or in combination with other publicly available information, reveals the individual's identity. PHI includes medical information; patient billing and health insurance information; and applies to a patient's past, current or future physical or mental health or treatment.

"Restricted Information" or "RI" (as defined by UC Policy IS-3, Electronic Information Security) describes any confidential or Personal Information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. This includes Personal Information, PHI and ePHI as defined in this section but could also include other types of information such as research data.

"System Development Life Cycle (SDLC)" is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal. There are many different SDLC models and methodologies, but each generally consists of a series of defined steps or phases.

"IT Resources" (as defined by UC Policy IS-3, Electronic Information Security) is a term that broadly describes IT infrastructure, software and/or hardware with computing and networking capability. This includes both UC-owned and personally owned devices while they store Protected Health Information or Restricted Information, are connected to UC systems, are connected to UC Networks, or used for UC business.

STANDARD

1) Information security measures are most efficient and effective when they are integrated into a system or application from the beginning of its development or implementation, rather than added on at the end of the process. Further, as the security needs of a project change throughout its development and life cycle, maintaining the desired level of protection requires periodic re-evaluation.

2) In order to protect UCLA Health Science's IT Resources and the data they contain and process, information security best practices shall be incorporated into all stages

of the development and implementation of new and upgraded systems and applications (henceforth referred to jointly as "systems"). This set of stages is known as the Systems Development Life Cycle (SDLC).

3) The SDLC encompasses the entire lifespan of a system, from conceptualizing through implementing and finally decommissioning. This standard focuses on a general overview of security integration into the SDLC, and does not prescribe or mandate any particular SDLC model or methodology.

4) This standard applies to all projects, large and small, which involve the creation or upgrading of one or more systems which use or interface with UCLA Health Sciences IT Resources. Additionally, this standard (in particular Stages 4 and 5 below, but also elements of the other stages where relevant and/or incomplete) applies to all existing and retiring systems, as securing a system is an ongoing process which should be an active part of system maintenance.

5) The list provided below provides a minimum set of information security-related activities for effectively incorporating security into a system. While the specific means of implementation will vary depending on the nature of the project, all development projects shall follow appropriate security best practices, including but not limited to:

<u>Stage 1: Planning, Requirement Gathering, and Analysis</u>

a) Determine the nature of the information which will be transmitted, stored, created, or modified by the system. Categorize the sensitivity of the information, and identify special handling requirements for sensitive information, such as PHI or RI.
b) Determine the threat environment in which the system will operate, and establish an initial description of the basic security/privacy needs and requirements in terms of confidentiality, integrity, and availability.
c) Review applicable UCLA Health Policies and Standards, including but not limited to HS Policy No. 9457, "Minimum Security Standards" and the Standards referenced in that document, as well as individual departmental standards and procedures, to determine which additional requirements apply.
d) Develop and incorporate security requirements into project specifications.
e) If outside parties are involved, evaluate their role and security capabilities to ensure that their security measures are sufficient and supported by the appropriate agreements.

<u>Stage 2: Design and Development</u>

All development work shall exhibit a separation between production and development/test environments.

Code should not be stored in an open or public-facing repository.

a) System development should go through the New Project Request (NPR) process.
b) Before a system goes live, it should go through the Risk Assessment process. (See HS Policy No. 9457, Minimum Security Standards – Health Sciences Risk Assessment Standard.) This process should begin as early as possible, and can begin prior to procurement.
c) Analyze the security requirement specifications in-depth.
d) Design the security architecture, selecting the appropriate security controls to address the identified security requirements for each component of the project.
e) Fully document the selected security controls as part of a system security plan document.
f) Develop awareness and training materials such as user manuals and operations/administrative manuals.
g) Design, develop, and implement the security controls as described in the security plan.
h) Frequently review the security controls throughout development, and as appropriate modify them to address changes to the initial system design. Document the modifications and the rationale for them, and update the security plan and other system documentation.

Stage 3: Integration, testing, and implementation

Real PHI and RI shall not be used for testing.

a) Develop a test plan, script, and scenarios, encompassing both functional and security testing, and appropriate to the scope, complexity, and anticipated implementation environments of the project.
b) Enable security control settings and protocols in accordance with, in order of precedence, UCOP, UCLA Health Sciences, and industry standard security implementation guidance.
c) Perform testing. Document all changes made to the security controls as a result of testing.
d) Remove all unnecessary test accounts, testing code, vendor access accounts, default passwords, etc. as soon as they are no longer needed.

Stage 4: Operation, Maintenance

a) Apply patches based on defined procedures.
b) Perform regular evaluation of any changes to the system and its surrounding environment in order to ensure adequate consideration of the potential security impacts of these changes.

c) Follow established change management and control processes.
d) Monitor and periodically test security controls to ensure that they continue to be effective in their application.

Stage 5: Decommission

a) Evaluate current legal and policy requirements for retention of data and logs. Make appropriate arrangements, ensuring that the retention method chosen accommodates future technology changes that may render other retrieval methods obsolete.
b) Ensure secure long-term storage of cryptographic keys for encrypted data.
c) Follow secure disposal/destruction practices appropriate for the type of data and equipment involved. These practices include deleting or overwriting the data, and/or physical destruction of the hardware when electronic means are insufficient.
d) Remove user and administrative access.

EXCEPTIONS

Any exceptions from this standard must be approved by the UCLA Health Sciences Chief Information Security Officer. The Chief Compliance Security Officer must be consulted when real patient data is to be used in development or testing environments.

QUESTIONS

1) For information on the UCLA Health project development and NPR process, please contact the UCLA Health Project Management Office.
2) If you have questions on Risk Assessment forms and processes, for assistance with technical issues, to request guidance on security best practices, or to request copies of the UCLA Health IT procedures related to this Standard, please contact the IT Security team (ITSecurityAll@mednet.ucla.edu).
3) To request an exception, please contact the Chief Information Security Officer.
4) For questions on this Standard, data categorization and handling requirements, or documentation and data retention requirements, please contact the Office of Compliance Services – Information Security (CompOffice@mednet.ucla.edu).

REFERENCES

HS Policy No. 9457, "*Minimum Security Standards*"

UCOP Secure Software Development Standard
https://security.ucop.edu/files/documents/guides/secure-software-development-standard.pdf

National Institute of Standards and Technology, SP 800-160 Vol. 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.*
https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final
University of California Records Retention Schedule
https://recordsretention.ucop.edu/

CONTACT

Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY

Created Date: September 5, 2019