TITLE: INFORMATION SECURITY RISK ASSESSMENT

PURPOSE: To ensure the prevention, detection, containment and correction of information security Violations that occur at Harris Health System Work Locations. This policy applies to all Harris Health System Workforce members and Business Associates using or accessing Harris Health System's information or information systems.

POLICY STATEMENT:

Harris Health System (Harris Health) will maintain an Information Security Risk Assessment program as a security standard for all Work Locations. This program will require implementation of standards and procedures to prevent, detect, contain and correct information security Violations that occur within Harris Health.

POLICY ELABORATIONS:

I. DEFINITIONS:

A. **BUSINESS ASSOCIATE:** A person or entity that provides certain functions, activities, or services for, to or on behalf of a Covered Entity involving the Use and or Disclosure of PHI as further defined in the HIPAA regulations.

B. **ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI):** PHI that is created, received, maintained or transmitted by electronic means.

C. **INFORMATION OWNER:** The person who has management responsibility for controlling the use and disposition of an application, record or database resource. The owner is, in many cases, external to Information Security or Information Technology.

D. **PROTECTED HEALTH INFORMATION (PHI):** Information that is created, received, transmitted or maintained by Harris Health in any form or medium, that relates to the patient's healthcare condition, provision of healthcare, or payment for the provision of healthcare, as further defined in the HIPAA regulations. PHI includes, but is not limited to, the following identifiers:

1. Name;

2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

    a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes.

E. **RISK**: A factor, event, element, or course that exposes Harris Health to liability, potential financial loss and/or data loss.

F. **RISK ANALYSIS:** A process whereby cost effective security measures may be selected by balancing the cost of the security measure against the losses that would be expected if the measure were not in place.

G. **RISK ASSESSMENT**: The process of assessing Risk, taking steps to reduce Risk and maintain an acceptable amount of Risk.

H. **SYSTEM ADMINISTRATOR:** The person who has responsibility for the operations of maintaining a computer system. Some operations include but are not limited to user account creation/modification/termination, system backups, and/or system configuration changes. These activities may be performed independent of, or in conjunction with, Harris Health Information Security and Information Technology.

I. **USER**: Any person who reads, enters, updates, sends, copies or prints information using any system regardless of the medium. Users must have an informational need to know, and must be authorized by the owner of the information.

J. **VIOLATION:** An infraction of a HIPAA policy, procedure or safeguard that may or may not result in damage to Harris Health or exposure to liability.

K. **WORKFORCE**: Harris Health Board of Managers, employees, Medical Staff, trainees, contractors, volunteers, and vendors.

L. **WORK LOCATION**: Any location where the information systems or resources of Harris Health can be accessed, created, received, maintained, or transmitted.

II. RISK ASSESSMENT:

A. Information Security will oversee Risk Assessment activities related to HIPAA Security.

B. At least annually, Information Security will work with Information Owners and System Administrators to conduct and document an accurate and thorough assessment of the threats and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) that Harris Health creates, receives, maintains, or transmits by:

1. Identifying and documenting where ePHI is stored, received, maintained, or transmitted through reviews of past or existing projects, interviews, documentation reviews, or other data gathering techniques as needed.
2. Assessing and documenting security measures in place to restrict threats from exploiting identified vulnerabilities to ePHI, determining the likelihood of the threat exploiting the vulnerability given the identified security measures, and determining the impact to Harris Health if the threat exploits the vulnerability given the identified security measures. This analysis will help assess the level of Risk across Harris Health.
3. Documenting assigned Risk levels and any corrective actions to be performed by Harris Health to mitigate each Risk level. This analysis will serve as a basis from which a sound Information Security Risk Assessment Program is developed and/or updated.

C. Note: Some risks pose minimal harm and may be considered acceptable with the review and approval of the Information Security Department. Other risk however may warrant further analysis to determine what mitigation, if any, would be required to reduce the Risk to an acceptable level. Vulnerabilities that are considered high Risk will warrant swift mitigation through the Information Technology Change Advisory Board.

D. The Information Security Department will monitor compliance with security policies and practices and will conduct on-going assessment of existing and planned information systems.

E. All identified Risks shall be documented and managed during their lifecycle. This would include identification, analysis, remediation and monitoring. The documentation may be reviewed periodically by the Information Security Department.

III. RISK CATEGORIES:

The Information Security Department will work with System Administrators, Information Technology, and other necessary Harris Health parties to address threats, vulnerabilities, and impacts on an ongoing basis.

A. The following Risk categories will assist in identifying the appropriate review path that a Risk will undergo to ensure identification, assessment, mitigation, and monitoring.

1. Harris Health Initiatives –system implementations, initiatives, or major system upgrades that are reviewed and approved by Information Technology Executive Committee (ITEC).
2. Operational Changes –changes to the production-computing environment that are part of the ongoing and day-to-day activities of information systems support teams.
3. Technical Vulnerabilities –technical aspects of securing the network environment from both external and internal unauthorized access and malicious attacks.
4. Isolated Security Incidents –reported instances of security policy Violations.

B. Each Risk shall be assessed according to each of the following categories to facilitate remediation planning.

1. Administrative – Administrative procedures to guard data confidentiality, integrity, and availability – these are documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data.
2. Physical – Physical safeguards to guard data confidentiality, integrity, and availability – these relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and other measures used to control access to computer systems and facilities.
3. Technical – Technical security services to guard data confidentiality, integrity, and availability – these include the processes that are put in place to protect and to control and monitor information access. Technical security mechanisms – these include the processes that are put in place to prevent unauthorized access to data transmitted over an internal or external communications network.
4. Organizational Practices – The practices include security and confidentiality policies, education and training programs, and sanctions.

5. Documentation – This includes all procedures, guidelines, standards and other appropriate documentation.

IV. RISK IDENTIFICATION:

A. For each of the those Risk categories identified by Harris Health, the responsibilities are assigned as follows:

1. The Information Security Department will be responsible for identifying Risks associated with Harris Health Initiatives and reporting those to the Architectural Review Committee as needed. Information Security Department will be responsible for identifying risks associated with operational changes and reporting those to the IT Change Advisory Board as needed.
2. The Information Security Department in conjunction with members of the network and server teams will be responsible for identifying and tracking the disposition of technical vulnerabilities.
3. Technical support personnel, Harris Health computer Users and Workforce members will be responsible for identifying and reporting Violations of the security policies to the Information Security Department. Once reported the Information Security Department will have responsibility for investigation and tracking the disposition of isolated security incidents.

B. Each Risk that is discovered within the computing environment will be documented and assigned to the appropriate Information Owner or technical resource for resolution. The Information Owner or technical resource will be held responsible for ensuring that the Risk is remedied or mitigated.

V. RISK ANALYSIS COMMUNICATION:

The Information Security Department will communicate identified Risks and make appropriate recommendations for remediation.

A. Information System Architectural Review Committee will review all aspects and Risks of new or upgraded system implementations. Information security will be

one of the aspects of system design, development and support that should be addressed by this committee.

B. Information Technology Change Advisory Board will review all aspects and Risks of changes to any system that may impact the production-computing environment. All changes will be requested of, and approved by, a change control committee that will review each request independently and then in aggregate to ensure that conflicts in changes are avoided.

C. The Information Security Department will review vulnerabilities that have been identified within the infrastructure of the Harris Health network. The Information Security Department will also have responsibility for reviewing isolated security incidents that have been reported by Harris Health work force members.

VI. RISK REMEDIATION:

Once a Risk has been identified and assessed, a remediation plan will be developed. The Information Security Department will involve appropriate parties, such as the Information Owner, technical resources, the County Attorney's Office, and the Office of Corporate Compliance as necessary. The Information Owner will document and implement additional security controls to reduce the Risk to acceptable levels or may opt to submit an exception request to document the reasons for not implementing an alternate control. The Information Security Department will review and approve or reject this request.

VII. RISK MONITORING:

The Information Security Department will have responsibility for ongoing reviews of security controls. This includes, but is not limited to the validation of mitigation plans that have been submitted to and approved by the Information Security Department.

REFERENCES/BIBLIOGRAPHY:

Harris Health System Policy and Procedures 3.11.800 Information Security

Harris Health System Policy and Procedures 3.11.805 Information Security Audit

Harris Health System Policy and Procedures 3.11.808 Information Security Awareness and Training

OFFICE OF PRIMARY RESPONSIBILITY:

Harris Health System Office of Corporate Compliance

REVIEW/REVISION HISTORY:

Record reviews and revisions below:

Effective Date	Version # (If Applicable)	Review or Revision Date (Indicate Reviewed or Revised)	Reviewed or Approved by: (If Board of Managers Approved, include Board Motion #)
04/20/2005	1.0	New	President/CEO
07/10/2006	1.1	Revised 06/20/2006	Harris Health Policy Review Committee
	1.2	Revised/Approved 05/13/2014	Operations Policy Committee