OSF HealthCare System Information Security Program

As it pertains to the Gramm Leach Bliley Act and the Health Insurance Portability and Accountability Act of 1996, Safeguarding of Electronic Customer Information and Protected Health Information

Objectives of the Information Security Program for the Gramm Leach Bliley Act (GLBA) and Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Ensure the security and confidentiality of customer information in compliance with applicable GLBA rules as published by the Federal Trade Commission.
- Provide administrative, physical, and technical safeguards to ensure compliance with the HIPAA Security Rule.
- Safeguard against anticipated threats to the security or integrity of protected electronic data.
- Guard against unauthorized access to or use of protected data that could result in harm or inconvenience to any customer.

Coordination and Responsibility for the Information Security Program

The Coordinator of the Information Security Program is the Chief Information Security Officer (CISO) for OSF HealthCare System. The Coordinator has also been designated as the HIPAA Security Officer. The Coordinator is responsible for the development, implementation, and oversight of OSF HealthCare's compliance with the policies and procedures required by the Gramm Leach Bliley Act (GLBA) Safeguards Rule and the Security Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Although ultimate responsibility for compliance lies with the Coordinator, representatives from each of the operational areas are responsible for implementation and maintenance of the specified requirements of the security program in their specific operation.

Risk Management Vs. Risk Avoidance

Information technology significantly influences the OSF mission of patient care, research, and outreach. Physicians and caregivers depend on the systems and services within the information enterprise to carry out their daily routine, record accomplishments and achievements, and help account for the revenue levels.

As discussed in NIST Special Publication 800-39, within an organization as diverse and complex as OSF, organizational risk consists of program management risk, investment risk, budgetary risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk. Security risk related to the operation and senior leaders, as part of their ongoing risk management responsibilities, will address use of information systems.

Effective security risk management requires that OSF departments and organizations operating in highly complex, interconnected environments using state-of-the-art and legacy information systems recognize that explicit, well-informed risk-based decisions help balance the benefits gained from the operation and use of these information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental disruptions, or human errors cause mission or business failure.

Managing information security risk, like risk management in general, is not an exact science. While based on the best collective judgments of individuals and groups, the concepts of risk avoidance, risk management and risk tolerance are not consistently understood or practiced. Risk avoidance is the elimination of hazards, activities and exposures that can negatively affect an organization's assets. Whereas risk management aims to control the damages and financial consequences of threatening events, risk avoidance seeks to avoid compromising events entirely.

As the OSF department responsible for cybersecurity; and in most of the information enterprise, day-to-day operations; the IT Security department takes a leading and advisory role in providing both the necessary and sufficient risk response measures to adequately protect the information systems. Tools and processes that seek to avoid risk increase the cost of operations and may impact the ability of clinicians and Mission Partners to carry out the mission. Likewise, risk-tolerant strategies place the organization at risk for cyber-attack, data loss or mismanagement, and increased cost through additional system administration and maintenance.

Optimized risk management is applied to data identified as Personally Identifiable Information (PII) or Personal Healthcare Information (PHI) that the organization requires for daily operations to include handling medical records, patient information, and employee records. With the widespread data sharing, analytics, and research involving healthcare and personal health information, we mconsider the impact of multiple and simultaneous incidents involving breach of data regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and subsequent legislation. Attention will also be directed toward financial and credit card or account information with handling regulated under the Purchase Card Industry Data Security Standard (PCI-DSS).

The Cybersecurity Strategy outlined in this document supports validation of effective practices, with automated real-time monitoring for accountability. Eventually, a set of decision metrics for estimating risk and security controls effectiveness will be developed. The entire OSF organization will benefit from being proactively involved and supportive of the continuous improvement offered within this strategy. For critical processes and systems, independent reviews will be planned and implemented to provide assurance that the spectrum of security controls are at the desired level of maturity and working as planned.

RISK ASSESSMENT

Risk assessment, the process of analyzing and interpreting risk, is comprised of three basic activities:

1. **Determine the Assessment's Scope and Methodology.** The first step in assessing risk is to identify the system under consideration, the part of the system that will be analyzed, and the analytical method including its level of detail and formality.

2. **Collecting and Analyzing Data.** The many different components of risk will be examined. This examination normally includes gathering data about the threatened area and synthesizing and analyzing the information to make it useful. The types of areas are:
   - *Asset Valuation.* These include the information, software, personnel, hardware, and physical assets (such as the computer facility). The value of an asset consists of its intrinsic value and the near-term impacts and long-term consequences of its compromise.
   - *Consequence Assessment.* The consequence assessment estimates the degree of harm or loss that could occur.
   - *Threat Identification.* A threat is an entity or event with the potential to harm the system. Typical threats are errors, fraud, disgruntled employees, fires, water damage, hackers, and viruses. Threats will be identified and analyzed to determine the likelihood of their occurrence and their potential to harm assets.
   - *Safeguard Analysis.* Safeguard analysis will include an examination of the effectiveness of the existing security measures.
   - *Vulnerability Analysis.* A vulnerability is a condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat.
   - *Likelihood Assessment.* Likelihood is an estimation of the frequency or chance of a threat happening. A likelihood assessment considers the presence, tenacity, and strengths of threats as well as the effectiveness of safeguards (or presence of vulnerabilities).

3. **Interpreting Risk Assessment Results.** The risk assessment produces a meaningful output that reflects what is truly important to the organization. The risk assessment is used to support two related functions: the acceptance of risk and the selection of cost-effective controls.

RISK MITIGATION

Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to management. Although there is flexibility in how risk assessment is conducted, the process of risk mitigation has greater flexibility than the sequence of events conducted in a risk assessment. The following activities are discussed in a specific sequence; however, they need not be performed in that sequence.

SELECT SAFEGUARDS

The identification of appropriate controls is a primary function of computer security risk management. In selecting appropriate controls, the following factors will be considered:

1) organizational policy, legislation, and regulation
2) safety, reliability, and quality requirements
3) system performance requirements
4) timeliness, accuracy, and completeness requirements
5) the life cycle costs of security measures
6) technical requirements
7) cultural constraints

ACCEPT RESIDUAL RISK

In consultation with other departments as necessary, the Chief Information Security Officer (CISO) will decide if the operation of the IT system is acceptable, given the kind and severity of remaining risks. The acceptance of risk is closely linked with the authorization to use an IT system, which is known as accreditation. Accreditation is the acceptance of risk by management resulting in a formal approval for the system to become operational. OSF uses an internal accreditation process that includes formal reviews completed by the Security Design Council, engaging the CISO where escalated, and also in matters involving business decisions OSF has instituted the Data Stewardship Workgroup.

IMPLEMENTING CONTROLS AND MONITORING EFFECTIVENESS

The safeguards selected need to be effectively implemented. To continue to be effective, risk management needs to be an ongoing process. This requires a periodic assessment and improvement of safeguards and reanalysis of risks.

OSF Compliance and Internal Audit has developed an audit program that is based on an organization-wide risk assessment. During the risk assessment and subsequent audit program, controls and systems are audited and monitored for effectiveness.

UNCERTAINTY ANALYSIS

In many cases, risk management relies on speculation, best guesses, incomplete data, and many unproven assumptions. An uncertainty analysis will be performed and documented so that the risk management results can be used knowledgeably. There are two primary sources of uncertainty in the risk management process:

1. A lack of confidence or precision in the risk management model or methodology
2. A lack of sufficient information to determine the exact value of the elements of the risk model, such as threat frequency, safeguard effectiveness, or consequences.

OSF's efforts will provide direction and, through the establishment of cybersecurity measures of effectiveness, emphasize continued identification of sensitive or restricted information. Efforts will include a management strategy including processes that prevent inappropriate access to or loss of sensitive or restricted data. This scope will include continued diagnostics using the right tools and access to all IT assets that ensure visibility of vulnerabilities and risk associated with their specific technology. Refining the processes and procedures to manage our intellectual property and other sensitive data will follow it.

IMPLEMENTATION OF POLICIES AND PROCEDURES

Questions regarding GLBA impacts on business processes and policies will be directed to the Coordinator of the Information Security Program, questions regarding HIPAA impacts on business processes and policies will be directed to the Chief Privacy Officer, and questions regarding technical issues, risk assessments, and information technology security policy will be directed to the Chief Information Security Officer.

OVERSIGHT OF SERVICE PROVIDERS AND CONTRACTS

GLBA requires OSF to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. OSF Legal Counsel has assisted with language to ensure that all relevant service provider contracts comply with GLBA provisions. Contracts will be reviewed to ensure the following language is included:

[Service Provider] agrees to implement and maintain a written comprehensive information security program containing administrative, technical and physical safeguards for the security and protection of customer information and further containing each of the elements set forth in § 314.4 of the Gramm Leach Bliley Standards for Safeguarding Customer Information (16 C.F.R. § 314). [Service Provider] further agrees to safeguard all customer information provided to it under this Agreement in accordance with its information security program and the Standards for Safeguarding Customer Information.

The GLBA contract due diligence is considered in various aspects of contract negotiation, including security control reviews.

Similarly, HIPAA allows a covered component to disclose protected health information to a business associate who is providing a particular function for the covered entity only if the covered entity obtains satisfactory assurances that the business associate will safeguard the information appropriately as required by HIPAA. Excluded from this requirement are disclosures for treatment, and other exceptions. Standard contracts have been developed by legal counsel. The covered component is responsible for identifying the need for a business associate agreement and will contact the Ministry Privacy Officer to determine if a business associate's agreement is required and for issuance of the agreement. Procurement Services may issue a business associate agreement in conjunction with a master agreement and will coordinate with the Chief Privacy Officer will this occur. These contracts will not be issued by covered components independently.

EVALUATION AND REVISION OF THE INFORMATION SECURITY PROGRAM

GLBA mandates that this Information Security Program be subject to periodic review and adjustment. The most frequent of these reviews will occur within Information Technology Security where constantly changing technology and constantly evolving risks indicate the wisdom of regular reviews. This Information Security Program is reevaluated annually in order to ensure ongoing compliance with existing and future laws and regulations.

ESTABLISHMENT OF INCIDENT RESPONSE PLAN

OSF has an Incident Response Plan in place which is reviewed on an annual basis by the Information Technology Department. The official OSF Incident Response Plan is available upon request.

QUALIFIED INDIVIDUAL REPORTING TO THE BOARD

The Chief Information Security Officer (CISO) reports to the OSF Board of Directors on a quarterly basis regarding the status of the Information Security Program.