**Scope**The HIC Information Security Program Charter and accompanying policies, guidelines, and procedures apply to all employees and contractors operating at HIC locations and subsidiaries including all users granted access to HIC information systems. The HIC Information Security Program (“Security Program”) applies directly to users handling, communicating, storing, administering systems involving protected health information (PHI) regulated by Health Insurance Portability and Accountability Act (HIPAA) including the standards for personally identifiable information (PII).

**Mission***“To provide a comprehensive approach for the administration of physical and non-physical components and systems to develop effective methods to support risk management objectives. The HIC Security Program aims to develop a strong security culture by affecting human attitudes and behavior to be in compliance with the Health Insurance Portability and Accountability Act (HIPAA), regulations associated with personally identifiable information (PII), and payment card industry (PCI) standards.”*

The policy guides employees to identify and follow rules set forth by HIPAA for health insurance companies for their respective business units and systems. Additionally, the policy enables a standard system for practices across HIC locations and subsidiaries to provide knowledge to staff, particularly new employees, on how processes are carried out. Furthermore, the policy serves an invaluable resource for documented guidelines to reduce human generated errors (InfoSec, n.d.).

The security program will protect information by developing policies to identify assets, categorize by business impact, and establish protection mechanisms for assets using a risk management approach (Palmer et al., 2000). The program will establish acceptable use of assets to be sourced from authoritative resources for health insurance companies.

Information system threats will be countered by the policies developed by the security program by way of identification, prioritization, monitoring, and response. Monitoring activities support risk management objectives by having a transparent information system for the administrator to locate, respond, and recover from threats on the network.
Monitoring activities will include the use of metrics and Cyber Threat Intelligence (CTI) to provide on-going assessment to obtain the state of the network. Monitoring metrics and CTI referenced in the policies, standards, guidelines, and procedures are intended to strengthen the strategic, operational, and tactical position of HIC and subsidiaries.

The policy aims to align with HIC’s security principles of:

**Least Privilege Principle**: Users and processes given the least authority and minimum access to resources required to accomplish a given task.
**Accountability Principle**: All significant system and process events should be traceable to the initiator.
**Minimum Dependence on Secrecy Principle**: Controls to still be effective even if an opponent knows of their existence and knows their mode of operation.
**Control Automation Principle**: Automatic controls should be used rather than controls which depend on human vigilance and human behavior.
**Resiliency Principle**: Systems managed to minimize damage in the event of breakdown or compromise.
**Defense in Depth Principle**: Layered controls involving backup or supporting mechanisms for primary controls.
**Approved Exception Principle**: Policy exceptions to always have management approval.
**Secure Emergency Override Principle**: Controls only bypassed in predetermined and secure ways.
**Auditability Principle**: An independent expert must be able to verify that the system conforms to the security policy.
(Sherwood, et al., 2005)

**Ownership:**All individuals identified in the scope of this Charter are responsible for familiarizing with the Information Security Program and complying with all applicable policies. Specifically, HIC management is accountable for the execution of the HIC Information Security Program and ensuring that policy is properly communicated to their respective employees and business partners. HIC management must assist and support the creation of sound policies, standards, guidelines, and procedures for their respective business unit to provide all-inclusive and wide-ranging security program. HIC managers and team leaders are to assist in any audit activities relating to the consistency of approved policies and procedures.

It is the responsibility of the Chief Information Security Officer (CISO) to establish an Information Security Awareness Program (ISAP) to ensure policies and procedures are communicated across all HIC business units. The CISO is responsible to match incoming components, system, software, and processes to be in alignment with the existing information security policy. CISO responsibilities may be granted to the following titles: Director of Information Security, Chief Security Officer, Director of Risk and Compliance, or Information Security Program Manager (Johnson, 2015).

The Chief Information Officer (CIO) is responsible for appointing the CISO, to manage the HIC Security Program, and for approving the Security Program policies. Any minor or material changes of the policy is not without approval by both CISO and CIO. The CIO takes full ownership and accountability of the HIC Security Program Charter (SPC) and accompanying policies, guidelines, and procedures.

The Chief Executive Officer (CEO) responsibilities include reviewing and approving the HIC SPC to align with the mission of HIC and its subsidiaries.

**Coverage:**
Failure to comply with HIC Security Program policies, guidelines, and procedures may result in termination. Management is recommended by the Security Program to take at least a three-step approach that includes verbal warning, written warning with copy submitted to the CISO, and a remediation action. The CISO is responsible to assess fair use and conformance to the HIC Security Policy and has the powers to reverse any decisions made by management involving the security program. The CISO and managers observing employee conformance to the policy should enforce rules to the same intensity as the impact of its violation. Violations include the failure to implement safeguards that reasonably and appropriately protect e-PHI (HHS.gov, n.d.).

Identified deficiencies in the security program should be communicated by any user of HIC systems to the CISO for immediate correction and reimplementation of the component, service, or system. Exceptions to the policy are not without explicit written consent by the authorized approval authority stated in the policies, standards, and guidelines.

Violations of the HIC Security Policy that can result in lawsuits are to be communicated by the CEO or CIO to the legal department to assess cost and recovery from lawsuits referencing applicable regulations and laws.

Creation and use of policy is used to support the HIC business mission and NOT to be used for offensive and/or hostile acts against an employee in the workplace. Unfair punishment reported and resulting from the security program will be assessed by either CISO or CIO. In any event a user of the security program feels they are being coerced to violate a program, procedure, law, or principled human right should report the incident to the CISO.

An annual review of the HIC Security Program will be conducted annually by the CISO under the time specified by the CEO or CIO. This includes a formal report submitted to the CIO comprising of compliance metrics and recommendations to improve the program. A review will be conducted after any significant changes to law and/or operating environment to assess the security program’s adequacy.

**Supplemental I: Policy Architecture**



**Supplemental II: HIC Policy Outline**

1. Network Security Policy
2. Platform Security Policy
3. Other Infrastructure Security Policies:

 General Infrastructure:

 Antivirus & Malware
 Remote Access Policy
 Acceptable Use Policy:
 User Authentication Policy:

 Specific Infrastructure:

Middleware Policy
Data Management Policy
Security Management Services Security Policy
Directory Service Security Policy

1. Application System Security Policies
2. Security Culture Development
3. Policy Management for Outsourced Strategy

 **Supplemental III: Hierarchical Committee Model for Information Security Management**



**Supplemental IV: State of the Current Policy**

Interviewer: Ryan Nye, Company**X**
Interviewee: Scott Aukerman, CEO

|  |  |
| --- | --- |
| **Interviewer Question** | **Interviewee Response** |
| Does the enterprise have any security policies at all? | *Yes* |
| Who developed them: an individual? A group? | *Our previous CEO outsourced policy formulation to an IT firm based out of India.*  |
| Where and how are the security policies available (paper, electronic)? | *We have the security policies available on paper, printed for new hires. For everyone else, they can use our intranet site to view the policy online.*  |
| When were the policies last updated? Last disseminated? | *Since I have started this position 8 years ago, the policy has not been updated. A recent audit report is prompting us to create a new formal policy to include recent technology, laws, and regulations.* |
| Who, if anyone, has explicit responsibility for maintaining security policies? | *Our security group and system administrators. But they are so bogged down with everyday tasks that it’s difficult for them to find time for re-writing a security policy.* |
| Who implements security policy at the enterprise level? | *The CISO* |
| To whom does the chief information security officer report within the enterprise? | *The CIO* |
| Who monitors compliance with security policies, standards, and compliance? | *The internal audit group* |

**Supplemental V: Resources to Establish Policy Framework**

|  |  |  |
| --- | --- | --- |
| **Organization**  | **Document** | **Description** |
| **Information Security Forum** | Information Security Forum releases the Standard of Good Practice for Information Security 2016 | *“All-in-one guide used by global organizations as their primary* *reference for information security best practices.”* |
| **International Standards Organization's Security Management series (ISO)****(ISO.org)** | The ISO/IEC 27000 family | “The ISO/IEC 27000 family of standards helps organizations keep information assets secure” (ISO, n.d.a). |
| ISO/IEC 27001 | *“ISO 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS)”*(ISO, n.d.a). |
| ISO/IEC 27002 | “*ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s)”* (ISO, n.d.b). |
| ISO/IEC 27005 | ““*ISO/IEC 27005:2011 provides guidelines for information security risk management…It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach”* (ISO, n.d.c). |
| **Information Systems Audit and Control Association's Control Objectives for Information Technology (ISACA)****(ISACA.org)** | COBIT 5 | *“COBIT 5 is the overarching business and management framework for governance and management of enterprise IT. This volume documents the 5 principles of COBIT 5 and defines the 7 supporting enablers”*(ISACA, n.d.). |
| **Suggestions from (Bayuk, 2016)** |

**Supplemental VI: Benefits of the Security Charter and Associated Documents**

Reasons for adopting the policy and associated framework is for the following:

|  |  |
| --- | --- |
| Internal Auditors | **Improved analysis** of risk in support of audit plans and reports |
| External Auditors | **Additional guidance** on exposure levels when establishing an opinion on the quality of internal control |
| Compliance | **Document support** for compliance requirements |
| General Counsel | **Document support** for regulation-related risk and potential impact or legal implications |
| Regulators | **Document support** for their assessment of regulated enterprise IT risk management  |
| Insurers | **Document support** for adequate IT insurance coverage and seeking agreement on exposure levels |
| Rating Agencies | **A document reference** to assess and rate objectively how an enterprise is managing IT risk (in collaboration with insurers) |
| IT Contractors and Subcontractors | **Better alignment of utility** **and warranty** of IT services provided**Understanding of responsibilities** in the risk environment context |
| Modified table from (ISACA, 2013) |

**References**

Bayuk, J. (2009, June 16). *How to Write an Information Security Policy.* Csoonline.com. Retrieved from https://www.csoonline.com/article/2124114/it-strategy/strategic-planning-erm-how-to-write-an-information-security-policy.html

HHS.gov. (2013, July 26). *Summary of the HIPAA Security Rule*. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Information Security Forum. (2016, March 4). *The Standard of Good Practice for Information Security 2016, Executive Summary*. Securityforum.org. https://www.securityforum.org/uploads/2016/07/SoGP-2016-Exec-Summary-FINAL-260716.pdf

ISACA. (2013). *COBIT 5, for Risk.* Isaca.org. Retrieved from https://www.isaca.org/COBIT/Documents/COBIT-5-for-Risk-Preview\_res\_eng\_0913.pdf

ISO. (n.d.a). *ISO/IEC 27000 family - Information security management systems.* ISO.org. Retrieved March 16, 2018 from https://www.iso.org/isoiec-27001-information-security.html

ISO. (n.d.b). *ISO/IEC 27002:2013* *Information technology -- Security techniques -- Code of practice for information security controls.* ISO.org. Retrieved March 16, 2018 from https://www.iso.org/standard/54533.html

ISO. (n.d.c). *ISO/IEC 27005:2011, Information technology -- Security techniques -- Information security risk management.* ISO.org. Retrieved March 16, 2018 from https://www.iso.org/standard/56742.html

Johnson, R. (2015). *Security Policies and Implementation Issues, Second Edition.* Burlington, Massachusetts: Jones & Bartlett Learning

Palmer, M.E., Robinson, C., Patilla, J., Moser, E.P. (2000)*. META Security Group Information Security Policy Framework, Best Practices For Security Policy in the Internet and e-Commerce Age.* Retrieved from http://horseproject.wiki/images/1/18/Information-Security-Policy-Framework-Research-Report.pdf

Sherwood, J., Clark, A., Lynas, D. (2005). *Enterprise Security Architecture, A Business-Driven Approach*. Boca Raton, Florida: CRC Press.

**Logo from:**

MarksMan Healthcare Communications. (n.d.). *HEOR – INDIA CONCLAVE (HIC).* Retrieved March 14, 2018 from https://marksmanhealthcare.com/heor-india-conclave/