ADMINISTRATIVE STANDARD
CATEGORY: Third Party Security Requirements
SUBJECT: Third Party Security Requirements

This Administrative Standard supports Ascension Administrative Policy #400, Information Security.

This Standard replaces and supersedes Ascension Administrative Policy #406, Third Party Security Requirements.

SUBJECT

This Standard defines the security requirements for Third Parties receiving, transmitting, accessing, and/or hosting Ascension Sensitive data or requiring access to Ascension Networks and/or performing business functions on behalf of or for Ascension. This includes, but is not limited to, Third Parties providing hardware, software, professional services, staffing services, or requiring software installation on Ascension Devices including Medical Devices.

DEFINITIONS

Application shall mean an executable software program, or group of programs, that is designed to deliver some or all of a series of steps needed to create, update, manage, calculate or display information for a specific business purpose.

Ascension shall mean Ascension and all organizations controlled by Ascension.

Ascension Information shall mean all records and data, regardless of format, created, received, disclosed or used in the course of Ascension business or on Ascension time or Ascension Systems, including, but not limited to, email, voicemail, text messages, paper documents, electronic documents and data, databases, application information, information on Ascension social media sites, such as Twitter and Facebook, Ascension intranet sites or external website postings, Ascension blog posts, or other electronic or photographic media. "Ascension Information" can include information maintained on a personal laptop, smartphone, cell phone, or mobile device, whether or not such device is connected to an Ascension System, including a Bring-Your-Own Device or "BYOD", if such information is created, received, or used in the course of Ascension business.

Ascension Organizations shall mean Ascension, Ascension Subsidiaries, and other subsidiary organizations in the Ministry, including but not limited to Ascension Healthcare Subsidiaries.

Availability shall mean the ability of an authorized person to use or access objects, resources, data, or information when needed, without undue delay.

Breach shall mean the circumvention or defeat of security controls which could result in a penetration of a system or network; or a violation of controls of a particular information system such that information assets or system components are susceptible to attacks which could adversely affect confidentiality, access, availability, and/or integrity of computer systems, components or data.

Business Associate shall mean an individual or organization who with respect to an Ascension Organization meets the definition of a business associate under HIPAA.

Business Associate Agreement shall mean a contract between a covered entity and a business associate meeting the requirements under HIPAA and entered into to ensure that the business associate will appropriately safeguard Protected Health Information. The Business Associate Agreement also serves to clarify and limit, as appropriate, the permissible uses and disclosures of Protected Health Information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate.

Cardholder Data shall mean that, at a minimum, cardholder data consist of the full personal account number. Personal cardholder data may also appear in the form of the full personal account number plus any of the following: cardholder name, expiration date and/or service code.

Confidentiality shall mean and include the property that data or information is not made available or disclosed to unauthorized persons or processes.

Data Backup shall mean the process of copying all electronic data to media for applications and computer systems for recovery purposes.

Device shall mean: (1) any piece of equipment used in computer input/output operations including but not limited to laptop computers, desktops, workstations, tablets, removable storage devices, card readers, servers, network components, printers, or any other mobile device; or (2) any medical device.

Disaster shall mean an event that would result in complete or near complete loss of computer systems or any event that creates an inability on an organization's part to provide critical business functions for some predetermined period of time.

electronic Protected Health Information (ePHI) shall mean and include all individually identifiable health information that is transmitted by or maintained in electronic media.

Encryption shall mean to modify or code data so that it is illegible without a specific key to decode it.

ePHI Application shall mean and include any application that creates, modifies, processes or stores electronic Protected Health Information.

Firewall shall mean a device that prevents unauthorized access to private data, including ePHI, by computer users outside of the Ascension Organization network.

HIPAA shall refer to the Health Insurance Portability and Accountability Act of 1996 and any amendments, regulations, rules, and guidance issued thereto and the relevant dates for compliance.

Integrity shall mean the property that data or information has not been altered or destroyed in an unauthorized manner.

Malicious Software shall mean the programs written and distributed with the intent to cause damage to or disrupt networks, systems, devices, servers and/or data, including, but not limited to viruses, worms, Trojan horses and email bombs.

Medical Device shall mean any instrument, apparatus, appliance, material or other article, whether used alone or in combination, together with any accessories or software for its proper functioning, intended by the manufacturer to be used for human beings in the:

1. Diagnosis, prevention, monitoring, treatment or alleviation of disease, injury or handicap;
2. Investigation, replacement or modification of the anatomy or of a physiological process;
3. and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means. (Source: "Institute of Clinical Research")

Mobile Device shall mean and include any portable computer/device that allows for storing, accessing and organizing digital information. This includes, but is not limited to, iOS (Apple iPhone/iPad), Android, Windows Phone, and other smartphone, tablet, laptop computers, removable storage devices, and other mobile device units, with this capability.

Network shall mean a group of interconnected (via cable and/or wireless) computers and peripherals that is capable of sharing software and hardware resources between many users.

Offshore shall mean any geographic location outside of the United States.

Payment Cards shall mean, for purposes of Payment Card Industry Data Security Standard, any payment card/device that bears the logo of the founding members of Payment Card Industry Security Standards Council. (American Express, Discover, MasterCard and Visa).

Payment Card Industry Data Security Standard (PCI DSS) shall mean the requirements set forth for payment card data security throughout handling, processing, transmission, and storage.

Personally Identifiable Information (PII) shall mean any data that could potentially identify a specific individual.

Personal Data shall mean any data that is subject to Privacy Laws.

Physical Safeguards shall mean physical measures, policies and procedures to protect an organization's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Policy shall mean high level statements that embrace Ascension's general beliefs, goals, objectives, and acceptable procedures for a specified subject area. Policies state required actions and may include pointers to standards. Policies require mandatory compliance.

Privacy Laws shall mean laws, states, regulations, rules, executive orders, directives, supervisory requirements in any jurisdictions worldwide, that relate to: (i) the confidentiality, collection, use, handling, processing, storage, security, protection, transfer or free movement of personal data, personally-identifiable information, customer information, or patient information; (ii) electronic data privacy; (iii) trans-border data flow; (iv) data protection; or (v) breach notification.

Procedures shall mean documented step-by-step instructions to accomplish specific tasks. Procedures may change frequently due to changes in systems, products, or business processes. Documented procedures help ensure that systems are implemented and maintained consistently across the organization. Procedures support standards in that they tell specifically how a standard will be implemented.

Public Network shall mean and include all systems, servers, routers and lines not owned or controlled by Ascension Organizations that can be accessed through public access methods, including dial-up, DSL, ISDN, cable, wireless and other connection methods.

Risk shall mean the possibility of suffering harm or loss.

Security Event shall mean any observable occurrence in a system or network with a potential negative consequence.

Security Incident shall mean the unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

Sensitive shall mean and include all information containing anything deemed confidential by an Ascension Subsidiary including ePHI, Cardholder Data, and Payment Card information.

Server shall mean a computer that provides data to other computers. It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet.

Standards shall mean specific approaches, solutions, methodologies, products, or protocols that must be adhered to in the acquisition, deployment, implementation, retirement, disposal or use of systems or system components. Standards are intended to establish uniformity for information system infrastructures, applications, procedures, or data.

System Owner shall mean the individual(s) who has been designated to carry accountability for an Ascension or Ascension Organization information system. A system owner may also be a data owner. (See also "Data owner".)

Third Party shall mean any entity not directly controlled by either the Ascension Organization or Ascension Technologies.

Third Party Subservice Organization shall mean an entity used by a Third Party to perform a subset of the services the Third Party provides to Ascension.

Third Party User shall mean and include the authorized individuals that routinely utilize Ascension information assets (i.e., applications, systems, networks and/or electronic data).

Workstation shall mean any electronic computing device, for example, a desktop computer or laptop, or any other device that performs similar functions, and electronic media stored in its immediate environment.

Third Party Security Requirements Standard

1. **General**

   1.1 Third Parties must have an information security Policy, with supporting Procedures in place that set forth how the Third Party will identify and manage its cyber security Risks.

   1.2 Third Parties must have clearly established accountability and ownership of their cyber security program. This should include assigned specific roles and responsibilities for the management along with proper staffing and financial resources.

   1.3 Third Party Users must be prohibited from making attempts to compromise or bypass Ascension Technologies security requirements.

   1.4 Background checks must be performed by Third Party prior to hiring all of its employees.

   1.5 Third Parties must have cyber Risk insurance coverage that provides financial mitigation to cyber Risk incidents and impacts. The amounts of this coverage may be detailed in the agreement between the Ascension Organization and the Third Party.

   1.6 Third Parties must remain compatible with the most recent Operating System version.

   1.7 Third Parties must immediately notify Ascension of employees or other personnel who were previously provided access to the Ascension Network or data and no longer need such access.

   1.8 Third Parties must follow a formal change management process.

2. Acceptable Use

2.1 Users must protect the Confidentiality, Integrity, and Availability of Ascension Organization systems and data entrusted to them and restrict their activities to legitimate business purposes only.

2.2 Under no circumstance is a Third Party User authorized to use Ascension Organization Applications, systems, Networks, and/or electronic data for activities that are illegal under applicable local, state, federal or international law.

2.3 Individuals who are not Associates and have been granted an email account are forbidden from using that email account to represent themselves as an Ascension Associate.

3. Application Security

3.1 Third Parties must restrict the use of unauthorized software and hardware through written policy.

3.2 Third Parties and Third Party Subservice Organizations storing, processing, or providing software that processes Ascension ePHI or Personal Data outside of the Ascension Network must provide, on an ongoing basis for the duration of the arrangement, periodic System and Organizational Controls ("SOC") 2, Type 2 reports or Health Information Trust Alliance Common Security Framework certification (HITRUST certification). The SOC 2, Type 2 or HITRUST certification requirement does not apply to disclosure of ePHI or Personal Data to governmental agencies, law enforcement, public health authorities and others when required by law.

3.2.1 SOC 2, Type 2 reports must be prepared by a Certified Public Accountant and performed in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No.18, and including in scope, at a minimum, the Security Trust Services Principle. Such reports must cover at least a six-month period of time, be contiguous in nature (i.e., containing no time gaps in coverage between reports) and contain a favorable assessment of the Third Party's internal controls.

3.2.2 HITRUST Certified Assessment Reports must be prepared by a HITRUST Assessor. A letter of certification is required with a supporting attestation report at least biannually detailing the scope of the assessment, testing results and any corrective action plans. At a minimum, scope must include HIPAA Regulatory Risk Factors and other Risk factors as deemed appropriate through the Ascension Technologies assessment process.

4. Asset Security / Device and Media Control

4.1 Third Parties must have a data destruction process in place which includes paper shredding and the secure disposal for all electronic hardware.

4.1.1 Prior to disposal or redeployment of electronic Devices, Medical Devices or media that contain ePHI, Personal Data or other Sensitive data the Third Party must ensure that data cannot be recreated or recovered. Such erasure shall be in

accordance with all applicable laws and the recommendations documented in Special Publication 800-88 (Guidelines for Media Sanitation) of the National Institute of Standards and Technology, or its most recent publication providing guidelines for media sanitation.

4.1.2 Final disposition of electronic and/or Medical Devices must be documented. All assets (including internal and external storage, data, etc.) belonging to Ascension must be returned upon termination of the contract between the Third Party and the applicable Ascension Organization.

5. Audit Controls

5.1 Third Parties must have the capability to produce system and security logs in standard exportable format in near real time.

5.1.1 The content and level of detail included in the activity logs must be based on an assessment by the System Owner of events that are most likely to be correlated with Risks to the Confidentiality, Integrity, and Availability of the information contained in the system.

5.1.2 The auditing mechanisms should record information such as the User identification associated with the event, the program or command used to initiate the event, and the time and date of the event.

5.1.3 System Owners must log and monitor events or actions which include, but not be limited to, logon attempts (including failed), changes to security settings and parameters, User account changes (e.g., added, changed privileges, deactivated, deleted), password resets, and system activity reviews of ePHI Applications as defined by HIPAA and HITECH.

5.2 Third Parties must maintain a current enterprise-wide knowledge base of its Users, Devices, and Applications, including but not limited to software and hardware asset inventory, Network maps, Network utilization, and performance data.

6. Authorization and Access Management

6.1 Third Parties must tightly control and manage the use of administrative privileges and limit the number of accounts that require administrative privilege. This includes removing administrative access from all Users unless there is a valid business need.

6.2 Third Parties must establish and maintain processes for secure User authentication protocols including:

- control of User ID's and other identifiers
- a secure method of assigning and selecting passwords
- use of unique identifier technologies
- blocking access to User identification after multiple unsuccessful attempts to gain access or the limitation placed on access for a particular system.

6.3 Third Parties must apply strong authentication mechanisms to manage User identities and access including:

- unique ID's,
- minimum password length,
- password complexity,
- history to a minimum of 5 past passwords,
- a required password reset at least every 365 days.
- Multi-factor authentication technology must be used to safeguard authentication attempts when technically feasible.

6.4 Third Parties must limit access to Ascension Systems and data, to authorized individuals with a valid business need.

7. **Business Associate Agreements**. Business Associate Agreements must be entered into between the applicable Ascension Organization and any Third Party that meets the definition of a Business Associate.

8. **Confidentiality and Non - Disclosure Agreements.** Confidentiality or Non–Disclosure Agreements must be entered into between the applicable Ascension Organization and any Third Parties who create, receive, access, maintain or transmit other, non-ePHI, Sensitive or proprietary data on behalf of Ascension Organizations. This requirement is met by entering into an agreement with such Third Party that includes a Confidentiality obligation that would govern this scope.

9. **Contingency Operations.** Third Parties must have an overall contingency plan and supporting Procedures for responding to an emergency that compromises the Confidentiality, Integrity and/or Availability of ePHI, Personal Data or other mission critical or Sensitive data contained in their environment. The contingency Plan must include:
   - Data Backup and recovery
   - Periodic impact analysis (e.g., business impact analysis or system criticality analysis)
   - Disaster recovery plan
   - Emergency mode operation plan to enable continuation of critical business processes for protection of the security of ePHI, Personal Data or other mission critical, Sensitive, or proprietary data while operating in emergency mode
   - IT business continuity Procedures so person, patient, resident, and client care can be continued effectively in the event of emergency situations, addressing both external and internal Disasters
   - Procedures for periodic testing and revision of the overall contingency plan.

10. **Data Backup and Storage** Third Parties must establish and implement Procedures to create, maintain and verify exact copies of Ascension data, including but not limited to ePHI, Personal Data and Sensitive information, based on criteria including but not limited to patient care impact, government regulation, business operations and security best practices. Data custodians must ensure back data is stored in a secure manner and must be available in the event of a system failure or other Disaster.

11. **Data Classification.** Security mechanisms for storage, transmission, handling, and destruction must be implemented to have a direct correlation with the Third Party's classification of the data. Third Parties must implement appropriate security measures that correspond with the classification of the data when technically and operationally reasonable. Third Parties are to provide their classification policy upon request.

12. **Facility Access Controls.** Third Parties must have facility access controls that include but are not limited to: storage of all Servers and Network electronics in environmentally safe and secure areas, maintenance of documented Standards and Procedures for gaining access, and maintenance of access controls and logs of access.

13. **Geographic Limitations**

    13.1 Ascension ePHI, Personal Data and other Sensitive data may not be stored or processed in any Offshore location and must remain within the 50 United States.

    13.2 Offshore access to Ascension ePHI, Personal Data or other Sensitive data may be allowed for support services such as help desk support, database support, troubleshooting, and pre-authorized critical business process support, and must meet the following criteria:

    13.2.1 Offshore resources accessing Ascension data must be approved by the Office of Ascension Chief Information Security Officer including but not limited to the means of accessing Ascension data and network.

    13.2.1.1 Offshore resources accessing Ascension data must be controlled by a technical platform that prevents downloading, printing, or exporting data to Devices located Offshore.

    13.2.1.2 Offshore access permitted must be contractually documented, including the purpose and the approved means of access.

    13.2.1.3 Offshore access permitted must be contractually documented, including the purpose and the approved means of access.

    13.2.2 Third Parties employing Offshore resources must demonstrate ongoing, unqualified SOC 2, Type II audits with the initial report dated within the last 12 months or a HITRUST certification within the last 24 months.

    13.2.2.1 United States based Third Parties employing Offshore resources accessing Ascension data must provide a current SOC 2, Type II audit or HITRUST certification that includes the Offshore resources.

    13.2.2.2 Offshore Third Parties accessing Ascension data must provide a current SOC 2, Type II Report or HITRUST certification that includes all Offshore resources.

14. **Incident Handling, Tracking and Response**

    14.1 Third Parties must have documented Procedures for monitoring, analyzing and responding to cyber Security Incidents and reviewing the cyber security Risks.

14.2 Third Parties must have a notification policy for Breaches, Security Events and Security Incidents. Third Parties must immediately report Breaches and suspected or verified Security Events, Security Incidents or Policy violations to Ascension Information Security or appropriate Ascension Organization management.

15. Installation and Configuration

15.1 For all products requiring Ascension Technologies installation, all Transport Control Protocol (TCP) and User Datagram Protocol (UDP) ports and services not required for product use will be removed prior to installation.

15.2 For all products requiring Ascension Technologies installation, all TCP and UDP ports and services not required for product use will be removed prior to installation.

15.3 Third Parties installing products on the Ascension network must agree to change the IP address or Network configuration of a Device or system component at Ascension's request without charge.

15.4 All software and installation media not specifically required for the product, including files, scripts, messaging services and data will be removed from the product following installation.

16. Integrity. Third Parties are required to protect ePHI from improper alteration or destruction. Ascension Technologies must approve any mechanism to be utilized to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

17. Malicious Software, Anti-Virus, and Encryption

17.1 Third Parties must implement the following security tools: endpoint protection, authentication, Firewall, antivirus, spam filtering, intrusion detection and prevention, Encryption, and Mobile Device Encryption.

17.2 Any Third Party-owned systems present on Ascension Networks (or Mobile Device used by Third Parties attached to the platform or backup Devices), must have full disk Encryption and removable storage Encryption installed and enabled with an Ascension Technologies-approved Encryption solution.

17.3 Third Party supported electronic Devices (including business equipment and Medical Devices) must be protected with current security patches and approved endpoint protection solutions or be isolated from the Ascension Organization's Network.

17.4 The Third Party must have a process to obtain, test and automatically deploy security patches and updates in a timely manner based on Risk. This process will confirm successful deployment and resolve update failures.

18. **Perimeter Defense** Third Parties must conduct regular internal and external vulnerability scans testing for client, Server, and Network infrastructure and implement processes to prevent, manage, mitigate, and remediate identified vulnerabilities.

19. **Regulatory Compliance** Third Parties must be able to demonstrate compliance with industry standards, all applicable Privacy Laws including HIPAA and any applicable Payment Card Industry Data Security Standards.

20. **Remote Access**
    - 20.1 Establishing a remote connection to or through an Ascension Organization Network from a Public Network requires the use of an Ascension Technologies-approved secure remote access method.
    - 20.2 Any attempt to bypass or compromise information systems security Procedures is prohibited.

21. **Risk Assessments** Third Parties must have a process to conduct regular and comprehensive cyber security Risk assessments. Results of the cyber Risk assessment as well as any action plans necessary to fully implement any required control points that have not yet been achieved shall be summarized and provided to Ascension.

22. **Workstation Security** Physical Safeguards must be implemented to restrict access to only authorized users. Workstations in areas that are vulnerable to theft must be protected using appropriate protection Procedures and anti-theft technologies.

23. **Security Awareness and Training** Cyber security awareness and training must be provided by Third Parties to all its employees and other personnel providing products or services to Ascension. At a minimum, Third Parties must be able to provide detailed reports validating individual training on an annual basis.

Effective Date: 10/21/2021 Revised Date: _____

Approved by: Title: Ascension Chief Information Security Officer and HIPAA Security Officer

Document Revisions

Version	Date	Author	Remarks
1.0	04/30/2018	Regional Security Officers	Original Issue
2.0	10/12/2021	Regional Security Officers	Required Refresh