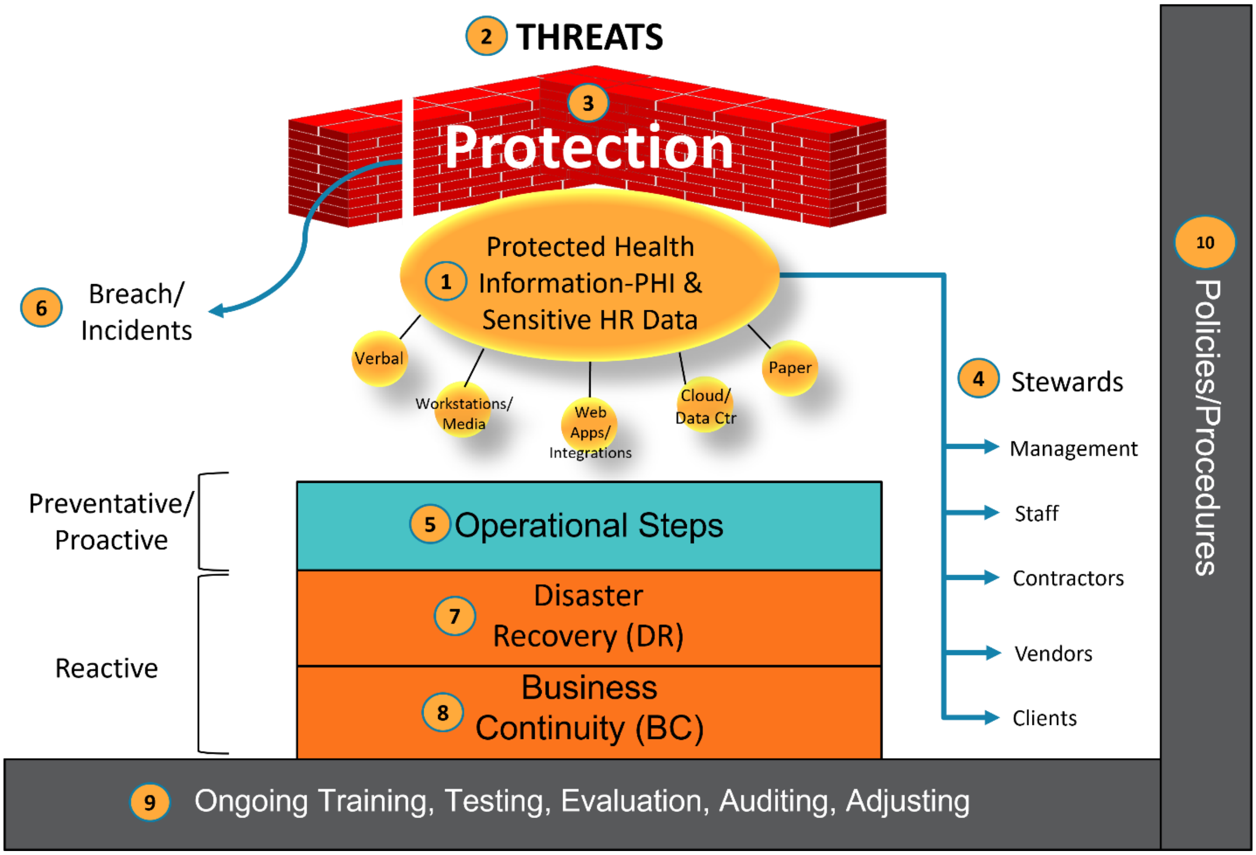
TAP Innovations
Security Program
Policies and Procedures

Version 2023-01-31

Table of Contents

TAP’s Security Program Protecting Healthcare, Financial and Other Sensitive Information

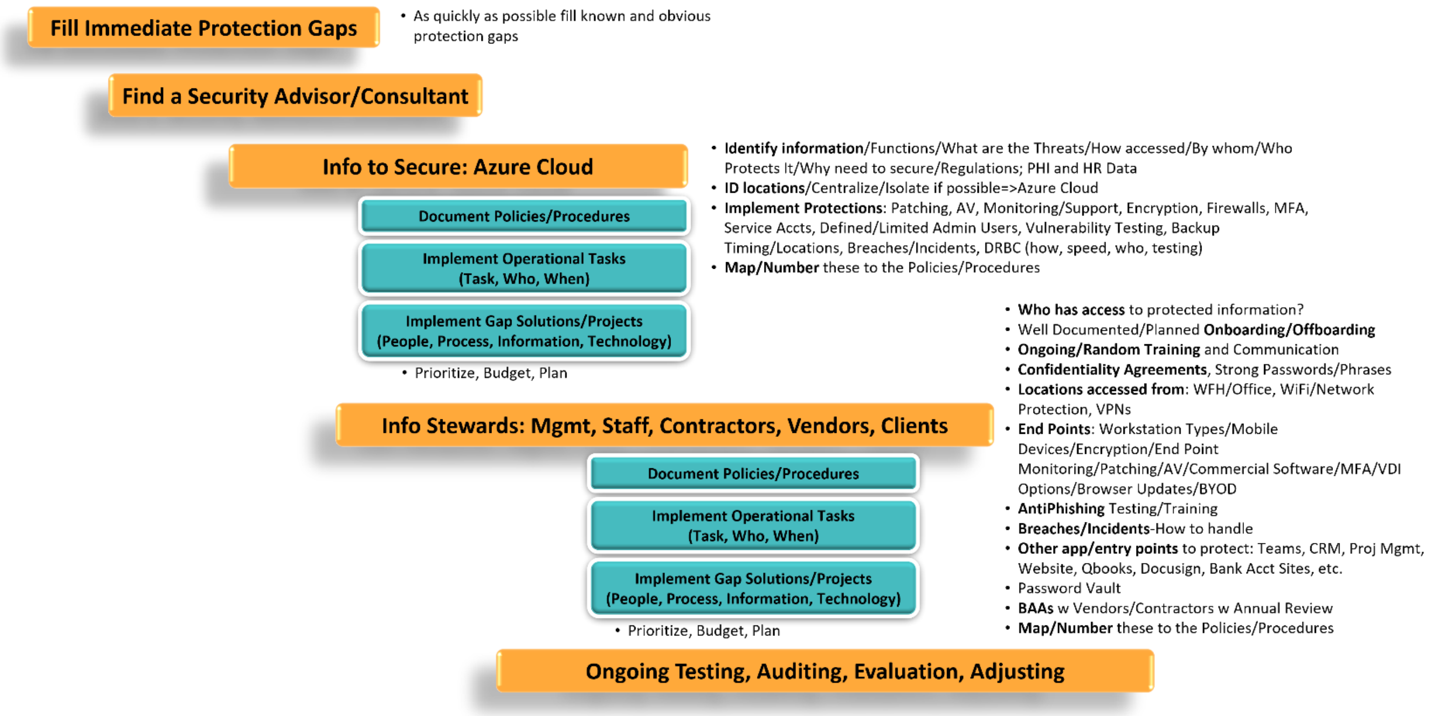


The threat environment is growing, and cybercriminals are becoming more sophisticated. They’re utilizing threat tactics that have made it increasingly difficult for organizations to protect themselves at scale. Cybercriminals are putting pressure on businesses by increasing the volume of these kinds of targeted attacks.

No matter how good our intentions are, we can make poor decisions at times. We need to make certain every team member always keeps security awareness as our focus, every day. We cannot let social status, time constraints, urgency, or seemingly legitimate requests make us vulnerable to attacks. The bad guys are always at work and are everywhere. They want access to sensitive information like patient data and social security numbers because they can make money from it. They will try to trick you to get it by asking for your login information for example. We must be diligent at all times to keep our clients and ourselves protected.

Back to Table of Contents

Implementation of TAP's Security Program



Fill Immediate Protection Gaps

- As quickly as possible fill known and obvious protection gaps

Find a Security Advisor/Consultant

Info to Secure: Azure Cloud

- **Identify information**/Functions/What are the Threats/How accessed/By whom/Who Protects It/Why need to secure/Regulations; PHI and HR Data
- **ID locations**/Centralize/Isolate if possible=>Azure Cloud
- **Implement Protections**: Patching, AV, Monitoring/Support, Encryption, Firewalls, MFA, Service Accts, Defined/Limited Admin Users, Vulnerability Testing, Backup Timing/Locations, Breaches/Incidents, DRBC (how, speed, who, testing)
- **Map/Number** these to the Policies/Procedures

Document Policies/Procedures

Implement Operational Tasks (Task, Who, When)

Implement Gap Solutions/Projects (People, Process, Information, Technology)

- Prioritize, Budget, Plan

Info Stewards: Mgmt, Staff, Contractors, Vendors, Clients

- **Who has access** to protected information?
- Well Documented/Planned **Onboarding/Offboarding**
- **Ongoing/Random Training** and Communication
- **Confidentiality Agreements**, Strong Passwords/Phrases
- **Locations accessed from**: WFH/Office, WiFi/Network Protection, VPNs
- **End Points**: Workstation Types/Mobile Devices/Encryption/End Point Monitoring/Patching/AV/Commercial Software/MFA/VDI Options/Browser Updates/BYOD
- **AntiPhishing** Testing/Training
- **Breaches/Incidents**-How to handle
- **Other app/entry points** to protect: Teams, CRM, Proj Mgmt, Website, Qbooks, Docusign, Bank Acct Sites, etc.
- Password Vault
- **BAAs** w Vendors/Contractors w Annual Review
- **Map/Number** these to the Policies/Procedures

Document Policies/Procedures

Implement Operational Tasks (Task, Who, When)

Implement Gap Solutions/Projects (People, Process, Information, Technology)

- Prioritize, Budget, Plan

Ongoing Testing, Auditing, Evaluation, Adjusting

How do we implement a practical security program for TAP?

First, we assign a Chief Information Security Officer and Privacy Officer. A CISO is responsible for technical security. A Privacy Officer is responsible for physical security.

Then, comes the Security plan. Sometimes you can develop a strategy and over time implement it. However, sometimes there are things to implement immediately in the security world. For example, if there is already a ransomware attack, you must act quickly and might not have time to develop a plan over several months.

The next thing we can do is bring client healthcare and client HR data into one environment and operate in a protective cloud. This draws a box around where information is kept, and provides a strong, updated and secure environment. It's critical to know answers to these questions: What is the information we are protecting?, What are the threats to that particular information?, How it is accessed and by whom?, and Who protects it?. We have to ask ourselves why do we need to secure it and what are the regulations around that. By asking these questions, we get a list of protections or things to do like patching for viruses and malware, monitoring support, encryption, and firewalls.

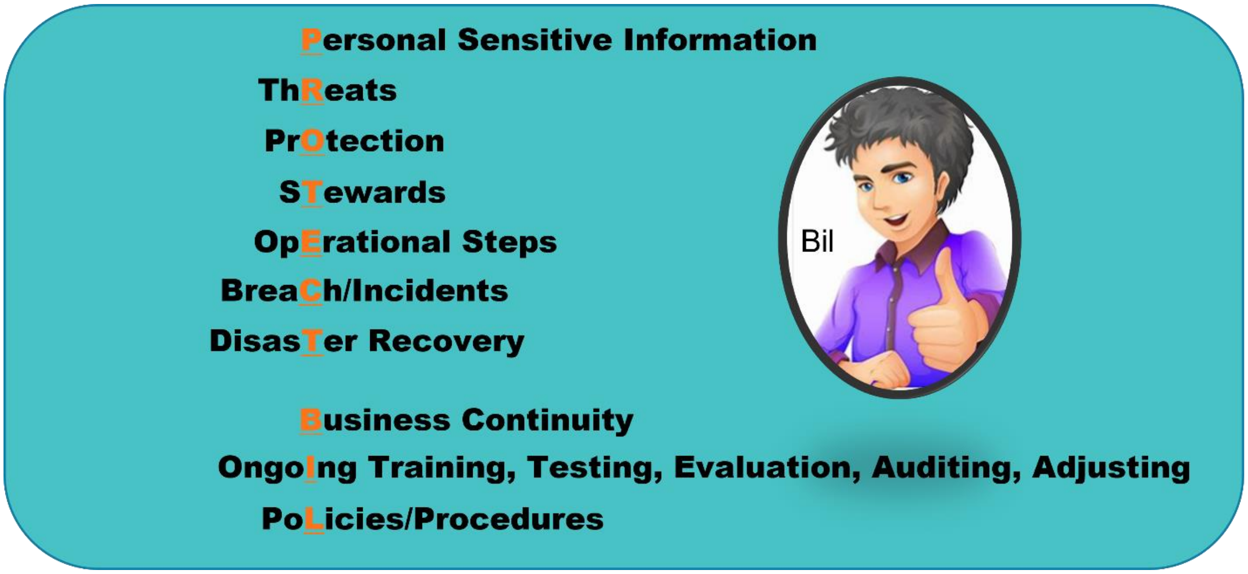
Next, we need to organize our policies and procedures so we can communicate to everyone from senior leaders, staff, contractors, and vendors—or all the key stewards of data. We need everyone to operationalize these policies and procedures and these need to be woven in day-to-day activities. These need to be assigned, tracked, and verified that they are being completed.

Then we evaluate the stewards of data. Who should have access to the protected information? There should be a well-documented planned onboarding and off-boarding process in place to make sure only the appropriate people have access to that particular information. We can't open access up to everybody. We must make sure the access is turned off when people are terminated or leave the company.

Back to Table of Contents

TAP's Security Program – PROTECT BIL

TAP has developed its enterprise security program using a top 10 list. This list provides a great framework for keeping clients and the organization safe. We can remember this list with the acronym PROTECT BIL.



Personal Sensitive Information

ThReats

PrOtection

STewards

OpErational Steps

BreaCh/Incidents

DisasTer Recovery

Business Continuity

OngoIng Training, Testing, Evaluation, Auditing, Adjusting

PoLicies/Procedures

Back to Table of Contents

1: Personal Sensitive Information

At TAP we protect personal sensitive information or SI (see definitions below). We have healthcare clients, and we are also working with client sensitive HR data. There are multiple areas where that information or data exists. These areas could be verbal, workstations, web apps, integrations, cloud/data center, and/or paper.

Some **key terms** used in this document:

Health Insurance Portability and Accountability Act (HIPAA)—(that's with one 'P' and two A's; it is commonly misspelled HIPPA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. There are two types of organizations that need to protect data.

- **Covered Entities (CE)**—These are healthcare providers. They provide direct health care services to patients. We are not a covered entity and do not have to comply with covered entity policies.
- **Business Associates (BA)**—TAP is considered a business associate and we support covered entities. That means we have access to their data and must comply in different ways to protect client health information. This is a key reason we have a security program to bring awareness to this situation.
- There are also 2 types of HIPAA safeguards:
  - **Technical safeguards**--the technology and the policy and procedures for its use that protect electronic sensitive information and control access to it.
  - **Physical safeguards**—these are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Protected Health Information (PHI) —The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. The electronic form of this is called ePHI.

Sensitive Information (SI)—is a term to refer to ALL data that must be guarded from unauthorized access and unwarranted disclosure to maintain the information security of an individual or organization. This is how we will refer to information throughout this document. It can include PHI, HR sensitive data such as social security numbers, and sensitive financial data like credit card information. The electronic form of this is called eSI.

Back to Table of Contents

2: Threats

The next thing to do is to really understand the threats and who are the bad guys and gals and what are the methods they use.

There are literally thousands of breaches every year across all industries. Some of the largest breaches "were caused by external cyber-attacks that leveraged phishing, malware, technical vulnerabilities, and more." In 2018, Marriott found a security breach in its Starwood Hotel branch that exposed 387 million guest records, including names, birth dates, gender, addresses, and passport numbers. Marriott said it wasn't sure how the breach occurred, and that it could have begun as far back as 2014.

Facebook's massive security breach has been well documented. The root of the September 2018 breach was bad code, according to some reports. Two bugs found in a privacy tool, and one in Facebook's video upload software, both led to the theft of usernames, gender, email addresses, location check ins, and relationship statuses.

Key Definitions:

Threat: the potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as:

- Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
- Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
- Natural – fires, floods, electrical storms, tornados, etc.
- Technological – server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
- Other – explosions, medical emergencies, misuse or resources, etc.

Threat Source – Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental which can impact the organization's ability to protect ePHI.

Threat Action – The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).

Back to Table of Contents

Risk Management

This policy establishes the scope, objectives, and procedures of TAP's information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission.

1. It is the policy of TAP to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of its sensitive information and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the organization's information security program.
2. Risk analysis and risk management are recognized as important components of TAP's corporate compliance program and Information Technology (IT) security program in accordance with the Risk Analysis and Risk Management implementation specifications within several standard security rules like HIPAA.

   A. Risk assessments are done throughout IT system life cycles:
      i. Before the purchase or integration of new technologies and changes are made to physical safeguards;
      ii. While integrating technology and making physical security changes; and
      iii. While sustaining and monitoring of appropriate security controls.

   B. TAP performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of eSI.

3. TAP implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
   A. Ensure the confidentiality, integrity, and availability of all eSI the organization creates, receives, maintains, and/or transmits,
   B. Protect against any reasonably anticipated threats or hazards to the security or integrity of eSI,
   C. Protect against any reasonably anticipated uses or disclosures of eSI that are not permitted or required, and
   D. Ensure compliance by workforce.

4. Any risk remaining (residual) after other risk controls have been applied, requires sign off by TAP's CISO/PRIVACY OFFICER and Senior Management Team.
5. All TAP team members are expected to fully cooperate with all persons charged with doing risk management work. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation according to TAP's Sanction policy.
6. All risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for six years.

Key Definitions

<u>Risk:</u> The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of eSI, other confidential or proprietary electronic information, and other system assets.

<u>Risk Management Team:</u> Individuals who are knowledgeable about the Organization's Security policies, procedures, training program, computer system set up, and technical security controls, and who are responsible for the risk management process and procedures outlined below. This team is generally comprised of the CISO/Privacy Officer, Physical Plant Security Officer, Systems Analyst(s), Privacy Officer, Risk Manager, Compliance Officer, Chief Information Officer, and Security/Technology subject matter experts.

<u>Risk Assessment:</u>

- Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place;
- Prioritizes risks; and
- Results in recommended possible actions/controls that could reduce or offset the determined risk.

<u>Risk Management:</u> This refers to two major process components: risk assessment and risk mitigation. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).

<u>Risk Mitigation:</u> A process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.

<u>Vulnerability:</u> A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.

Procedures

1. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of TAP's CISO/Privacy Officer (or other designated employee), and the identified Risk Management Team.
2. **Risk Assessment:** The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

   A. Step 1. System Characterization

      i. The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI is created, received, maintained, processed, or transmitted. Using informationgathering techniques, the IT system boundaries are identified, as well as the resources and the information that constitute the system. Take into consideration policies, laws, the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media). (See "Risk Analysis & Risk Management Toolkit – Network Diagram Example and Inventory Asset List" to assist with these efforts)

ii. *Output* – Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundaries.

B. Step 2. Threat Identification

i. In this step, potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. Consider all potential threat-sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats. The list should be based on the individual organization and its processing environment. (See "Risk Analysis & Risk Management Toolkit –Threat Overview" for definitions and the " Threat Source List" in the Risk Assessment for examples of threat sources.)

ii. *Output* – A threat statement containing a list of threat-sources that could exploit system vulnerabilities.

C. Step 3. Vulnerability Identification

i. The goal of this step is to develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network. (See "Risk Analysis & Risk Management Toolkit – Risk Assessment Template – Security Questions and Threat Source List".)

ii. *Output* – A list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources.

D. Step 4. Control Analysis

i. The goal of this step is to document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by the organization to minimize or eliminate the likelihood (or probability) of a threat-source exploiting a system vulnerability.

ii. *Output* – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.

E. Step 5. Likelihood Determination

i. The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls. (See "Risk Analysis & Risk Management Toolkit – Risk Likelihood, Risk Impact, and Risk Level Definitions".)

ii. *Output* – Likelihood rating of low (.1), medium (.5), or high (1). Refer to the NIST SP 800-30 definitions of low, medium, and high.

F. Step 6. Impact Analysis

i. The goal of this step is to determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to the organization's mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data. (See "Risk Analysis & Risk Management Toolkit – NIST Risk Likelihood, Risk Impact, and Risk Level Definitions".)

ii. Output – Magnitude of impact rating of low (10), medium (50), or high (100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

G. Step 7. Risk Determination

i. This step is intended to establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management (the mission owners) must take for each risk level. (See "Risk Analysis & Risk Management Toolkit – NIST Risk Likelihood, Risk Impact, and Risk Level Definitions".)

ii. *Output* – Risk level of low (1-10), medium (>10-50) or high (>50-100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

H. Step 8. Control Recommendations

i. The purpose of this step is to identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented. (See "Risk Analysis & Risk Management Toolkit – NIST - Risk Mitigation Activities".)

ii. *Output* – Recommendation of control(s) and alternative solutions to mitigate risk.

I. Step 9. Results Documentation

i. Results of the risk assessment are documented in an official report or briefing and provided to senior management (the mission owners) to make decisions on policy, procedure, budget, and system operational and management changes. (See "Risk Analysis & Risk Management Toolkit –Risk Analysis Report Template")

ii. *Output* – A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

3. **Risk Mitigation:** Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process to ensure the confidentiality,

integrity and availability of ePHI. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

A. Step 1. Prioritize Actions –
   i. Using results from Step 7 of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources.
   ii. *Output* – Actions ranked from high to low

B. Step 2. Evaluate Recommended Control Options –
   i. Although possible controls for each threat and vulnerability pair are arrived at in Step 8 of the Risk Assessment, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a “most appropriate” control option for each threat and vulnerability pair.
   ii. *Output* – list of feasible controls

C. Step 3. Conduct Cost-Benefit Analysis –
   i. Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.
   ii. *Output* – Documented cost- benefit analysis of either implementing or not implementing each specific control

D. Step 4. Select Control(s) –
   i. Taking into account the information and results from previous steps, the TAP’s mission, and other important criteria, the Risk Management Team determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI. These controls may consist of a mix of administrative, physical, and/or technical safeguards.
   ii. *Output* – Selected control(s)

E. Step 5. Assign Responsibility –
   i. Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.
   ii. *Output* – List of resources, responsible persons and their assignments

F. Step 6. Develop Safeguard Implementation Plan –

i. Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:
    a. Each risk or vulnerability/threat pair and risk level
    b. Prioritized actions
    c. The recommended feasible control(s) for each identified risk
    d. Required resources for implementation of selected controls
    e. Team member responsible for implementation of each control
    f. Start date for implementation
    g. Target date for completion of implementation
    h. Maintenance requirements.

ii. The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to the organization's executive management/leadership team (e.g. the Board, senior management, and other key stakeholders).

iii. Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations (often referred to as a work breakdown structure). Additionally, consider including items in individual project plans such as a project scope, a list deliverables, key assumptions, objectives, task completion dates and project requirements.

iv. *Output* – Safeguard Implementation Plan

G. Step 7. Implement Selected Controls – as controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.

i. Continually and consistently communicate expectations to all Risk Management Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.

ii. Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.

iii. If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.

iv. *Output* – Residual Risk

4. **Risk Management Schedule:** The two principal components of the risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of TAP's information security program:

A. Scheduled Basis – an overall risk assessment of TAP’s information system infrastructure will be conducted annually. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the corporate budgeting process.

B. Throughout a System’s Development Life Cycle – from the time that a need for a new information system is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.

C. As Needed – the CISO/Privacy Officer (or other designated employee) or Risk Management Team may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect TAP’s information systems.

5. **Process Documentation**. Maintain documentation of all risk assessment, risk management, and risk mitigation efforts for a minimum of six years.

Back to Table of Contents

3: Protection

Integrity of eSI – Protection

TAP shall appropriately protect the integrity of all eSI that is stored, processed, transmitted or received on business systems, networks or electronic resources from improper alteration or deletion.

TAP shall implement formal, documented process for appropriately protecting the integrity of eSI. At a minimum, the process shall include:

Access to delete or alter eSI is restricted to specified full access accounts. Authorized alterations or deletions are audited and reviewed as part of the Audit Policy. Such access and use shall be clearly defined and documented, and periodically reviewed and revised as necessary. The integrity of eSI in transmission between any two systems will be assured by encryption. The integrity of eSI at rest will be assured with Checksums, Digital Signatures, and/or Hash Values.

By limiting full access controls, user error or intentional improper alteration or deletion can be reduced to minimal possible extent.

By implementing encryptions for all eSI in transmission, integrity is automatically validated by the encryption transmission process over TCP/IP networks, validating the sequence and protected the content of each packet of information that is transmitted or received. Back to Table of Contents

Integrity - Mechanism to Authenticate eSI

TAP will take steps to ensure that, when reasonable and appropriate, electronic mechanisms are implemented to validate the integrity of eSI by proving that it has not been improperly altered or destroyed. Examples of electronic mechanisms that are capable of detecting and reporting unauthorized alteration or destruction of eSI include:

i. Checksum
ii. Hash values
iii. Digital signatures
iv. Encryption
v. Disk redundancy (such as Redundant Arrays of Inexpensive Disks or "RAID")

The use of electronic mechanisms to ensure that eSI has not been altered or destroyed will be determined by the CISO/Privacy Officer. Back to Table of Contents

Transmission of eSI/Encryption

There are various methods of encryption available to protect eSI from unauthorized disclosure while being transmitted across networks. Secure Socket Layer (SSL) encryption protects the transmission of protected health information, when implemented on web content. Secure File Transfer Protocol (SFTP) can be implemented to protect file transmissions. Transport Layer Security (TLS) protects other forms of electronic transmission including e-mail communications. In addition to these application layer encryption options, there are network layer encryption options such as Wireless encryption, Internet Protocol Security (IPSEC) and encrypted tunnel options from virtual private networks (VPN). Due to the various methods by which eSI can be transmitted, it is important to select the best encryption method for the transmission method to ensure the confidentiality and integrity of eSI in transmission. Back to Table of Contents

Transmission - Integrity Controls

When appropriate encryption is implemented on a TCP/IP network integrity is achieved through the combination of TCP/IP flow controls and the encryption/decryption process. As such, eSI shall not be transmitted in or out of the perimeter defense of a local network without appropriate encryption to protect the integrity and confidentiality of the transmission. Back to Table of Contents

Transmission – Encryption Keys

In order for encryption to be an effective security solution to protect the confidentiality and integrity of eSI, the encryption keys must be protected from unauthorized disclosure. The CISO/Privacy Officer or appropriate delegate will ensure the protection of encryption keys are secured from unauthorized disclosure for any encryption that is managed or implemented by TAP Innovations. Encryption keys will be maintained in secure storage locations accessibly only by the CISO/Privacy Officer or appropriate delegate.

Back to Table of Contents

Workforce Security – Access

TAP Innovations will ensure appropriate access is granted to all authorized members in a manner that is consistent with the HIPAA or other compliance rule of minimum necessary access. TAP Innovations will make every effort to ensure members that are not authorized, do not have access to protected health information. Back to Table of Contents

Workforce Security - Authorization and/or Supervision

TAP Innovations will grant access to SI based on workforce member job functions and responsibilities. The CISO/Privacy Officer are responsible for the determination of which individuals require access to SI and what level of access they require through discussions with the individual's manager and or department head. Requests for access should be submitted to the program manager and/or CISO/Privacy Officer with an explanation of the user access requirements and justification. The request, approval and resulting action is to be documented.

Requests to controlled areas where eSI may be accessed will be handled in similar fashion and approval will be sent to the facilities manager or CISO/Privacy Officer for action and documented.

TAP Innovations will keep a record of authorized users and the rights that they have been granted with respect to eSI. The company will maintain a comprehensive matrix of how and to who rights are granted. Back to Table of Contents

Workforce Security - Workforce Clearance Procedure

TAP Innovations will establish clearance for access to eSI or areas were eSI may be accessed based on the workforce members' job title or roles and responsibilities using the job description and responsibilities table. Workforce members must have appropriate background checks on file prior to being authorized for access to eSI or areas where it may be accessed. Clearance will be documented with access authorizations for review and revalidation.

Revaluation

Documented requests, clearance and authorizations must be revalidated regularly but no later than the anniversary of the authorization. Revalidation will include confirmation of the workforce members current job title, roles, and responsibilities to validate their access to eSI or areas where it may be accessed is valid. Back to Table of Contents

Workforce Security - Establish Termination Procedures

Termination

TAP Innovations must terminate access to eSI when employment or other arrangements with the workforce member ends. At the end of employment or other arrangements, the hiring manager is required to notify the CISO/Privacy Officer to review access requests, clearance and authorizations and terminate access to eSI or areas where it may be accessed. Termination notice and access revocation must be documented to include timing, revocation of access control devices and deactivation of information systems access.

An exit interview, if possible, must be conducted that includes a discussion of privacy and security topics regarding eSI.

Job Change

TAP Innovations must terminate access to eSI or authorize a new request for access to eSI or areas where it may be accessed when a workforce member's job title changes. Requests will be submitted and authorized following the Authorization and Clearance procedures. Requests, clearance, and authorizations for job title changes must be documented for future revalidation.

Back to Table of Contents

Access Controls

TAP limits information system access to authorized users and/or "system accounts/service accounts" and applications acting on behalf of authorized users or automated system jobs. Information systems and networks have access and authentication controls which employ user ID and passwords unique to each individual user. User IDs and passwords, as a means of authentication, restrict user privileges on the system to only those files, applications, data, and system resources needed for that user's role. Access to TAP information and technology is permitted only on a need-to-know basis, and users shall be granted only the minimum access rights and privileges needed to perform a particular function. Users are prevented from gaining access to information and technology for which they are not authorized.

Information Access will be restricted to authorized personnel based on approval for access and need to know or access specified levels of access.

Those with a need to know, but not a need to - or job role to enter or edit information - will be granted read only access to authorized information.

Those with a need to know and enter or edit information will be given Read/Write access to authorized information.

This is a need to read, write, modify, or archive information will be given Full Control. Full control is limited to authorized/specified administrative accounts and must be maintained on the administrative accounts log.

Access controls will be applied to each user account based on management approval and CISO/Privacy Officer authorizations. Accounts with access to systems or applications with eSI will be reviewed monthly.

Upon termination, please reference the Termination policy. Terminations should be processed within 24 hours of any workforce members' departure. Back to Table of Contents

Access Controls - Unique User Identification

All persons or entities requesting access to information systems must be positively and uniquely identified and authenticated before access is granted in order to provide unique accountability for the actions performed by the user.

Every user login must employ a user ID and password that uniquely identifies that user. Generic/Shared user IDs are not allowed. User ID credentials are granted only after access approval as specified in the Information Access Management Policy.

Accounts not associated with a specific user (e.g., service or machine accounts), must be protected from unauthorized use or disclosure.

All vendor-defined or system default IDs and passwords must be changed or deleted before the system is attached to TAP network. No user shall log into the network or system(s) anonymously (for example, by using a "guest" account). Back to Table of Contents

Access Controls - Emergency Access Procedure

Emergency access to electronic mediums may be granted on a need to know basis, provided the following requirements are met:

The CISO/Privacy Officer will initiate Emergency Access protocols and notify the business that Emergency Mode Operations have been activated.

Emergency Mode Access Requests must made by a manager-level or above employee;

While operating in Emergency Mode Operations - the CISO/Privacy Officer will approve all access requests

Emergency Mode access requests must be documented in the Emergency Access Request Log.

Emergency Mode access is made available for a 24-hour period, using unique authentication in order to preserve access audit and logging.

Once the emergency has passed, the CISO/Privacy Officer will announce the end of Emergency Mode Operations and resume normal access management. Back to Table of Contents

Access Controls - Automatic Logoff

If capable, applications that have the potential to contain eSI OR confidential data must be configured to automatically log off after **30** minutes of inactivity; and/or

Any device with an installed application that is not capable of automatically logging off after **30** minutes must be configured to automatically log the user off at the operating system level, or enact a passphrase protected screen saver after **30** minutes of inactivity;

To the extent possible, network and application credentials will be set to lockout after **3** consecutive failed attempts;

To the extent possible, network and application passphrases shall be set to expire every **90** days, and shall prevent users from utilizing the previous **5** passphrases.

If any such limitations are not supported by an application, the greatest possible restrictions allowable by said application for each item shall be enforced. Back to Table of Contents

Access Controls - Encryption and Decryption

Whenever possible, devices and media that contain or access eSI will be encrypted. Encryption methods may vary depending on device and media compatibility but must be documented in the eSI systems inventory. Cryptographic key management will be maintained in cryptography log, and shall be controlled and maintained by the CISO/Privacy Officer of appropriate administrative delegate. Back to Table of Contents

Facility Access Controls

TAP Innovations shall implement physical security controls that prevent unauthorized access to information systems and the facility or facilities in which they are housed. Because information is only as secure as the physical access to the systems on which it is house, this will include limiting access to buildings, facilities, offices, or rooms which house information systems used to access, store, process, or transmit eSI to those individuals authorized to access the information contained therein.

Prevention of access to information systems will be achieved by physical segregation from publicly accessible area of the business, and separation between back-office staff that are not authorized access to SI. Access to these systems will require authorization from the CISO/Privacy Officer and granted, only after authorization to access SI has been properly granted. Back to Table of Contents

Facility Access Controls - Contingency Operations

Facility access for the purpose of restoration of lost data will be provided at the approval of and by the CISO/Privacy Officer in support of the contingency and disaster recovery plans. All access granted for the restoration of lost data or in support of the contingency and disaster recovery plan shall be recorded and retained. Back to Table of Contents

Facility Access Controls - Facility Security Plan

All access to eSI is limited within the facilities. All users are assigned a unique user ID. Employees are not to share their user ID with anyone, at any time. This includes not using anyone's ID to access the premises, their access cards, keys, passwords, logins, or any other mechanism to access the facility or the resources contained therein which was not expressly approved and assigned to the individual.

An inventory of the facilities that house equipment that create, maintain, receive, and transmit eSI will be maintained. Likewise, an inventory of access authorizations and assigned access mechanisms will be maintained and reviewed every **12** months.

Facility access will be assured by implementing the following physical security safeguards:

☑ Access Badges

☑ Combination Keypads

☑ Locks and Keys

☑ Video Surveillance

The CISO/Privacy Officer will grant access to the facility(ies) and assign the corresponding access device(s) to authorized workforce member. Access authorizations will be inventoried and reviewed every **12** months. Back to Table of Contents

Facility Access Controls - Access Control and Validation Procedures

The CISO/Privacy Officer shall review and approve requests for access to facilities that house sensitive information. Access authorizations will be reviewed every **12** months and verified by the CISO/Privacy Officer. The CISO/Privacy Officer will document and retain review documentation including evidence of their involvement and attestation to the completeness and accuracy of the review.

Visitors must be checked-in and recorded in the visitor log. Visitors must be accompanied by authorized personnel at all times. Visitors must not be given access to information systems used to access, store, process, transmit or receive protected health information without prior approval from the CISO/Privacy Officer. The Visitor log must include the visitor's full name, reason for their visit, and the responsible workforce member that will supervise their visit. Back to Table of Contents

Facility Access Controls - Maintain Maintenance Records

TAP Innovations shall ensure all repairs or modifications to the facilities which impact security, are documented in the facility repair log. Facility repair log entries must include the date the repair or modification was first reported, the date the repair or modification was completed, a detailed description of the repair or modification, and the reason it affects the physical security of the facility. Items to be logged include but are not limited to required repairs or modifications to doors, walls, locks, hardware, windows, or other elements used to secure the facility and the information systems contained therein. Back to Table of Contents

Workstation Security - Workstation Use

Workstation Use

- Workstations should only be used by authorized Workforce members or vendor representatives following the requirements of the Facility Security Plan and Information Access Policies.
- Authentication to the client healthcare or HR data requires a unique user ID and password.
- Users are required to follow good security practices in the selection and use of passwords according to the Password Management policy.

Physical Placement and Monitoring

- Physical Workstation placement should minimize the possibility of unauthorized personnel viewing screens or data.
- Physical devices such as privacy guards will be utilized where needed to limit visibility of Confidential Information to unauthorized personnel.
- Workstations in high traffic areas used to Access Confidential Information must be monitored during business hours.
- Department managers are ultimately responsible for the physical placement and monitoring of Workstations in their areas.

Asset Documentation

- An inventory of all workstations used to access, store, process, transmit or receive confidential information will be maintained.
- Workstations that are to be retired or designated for disposal will be sanitized of all business software, licenses, and information - including but not limited to eSI and related software.
- Appropriate sanitization will be documented and confirmed by the CISO/Privacy Officer or designated workforce member.

Asset Management and Protection

- All Workstations purchased by TAP Innovations are considered company assets throughout the life of the asset.
- Workstations should not be relocated or changed by anyone other than authorized workforce members or vendors.
- Workstations shall be protected on and off the premises by employing: Security locks, alarms, or tracking devices will be appropriately used to physically secure Workstations in areas that are accessible to the general public.
- The User and department manager are jointly responsible for securing devices and ensuring compliance.
- Workstations that will be sent offsite for vendor maintenance will require an appropriate entity asset tracking form or service agreement, with the asset tracking details documented with the appropriate ticket tracking tool.

- Laptops and wireless device Users are expected to follow TAP policies, best practices, and industry standards to avoid laptop theft and/or breach of Confidential Information including but not limited to encryption of storage media, password protection, and the use of secure network connections.
- Good judgment and reasonable care should be exercised to avoid damaging equipment (e.g. do not drop the device or spill liquids on equipment).

Ethical Workstation

- Use Appropriate use of resources includes maintaining the security of the system, protecting privacy, and conforming to applicable laws, including Copyright and harassment laws.
- Workstations are to be used primarily for the conduct of business.
- Attempts to maliciously sabotage systems or networks using business resources are prohibited.
- Attempts to make a computer impersonate other systems, particularly via forged email, talk, news, etc., are prohibited.
- Users may not use their accounts to attempt to gain unauthorized Access to the organization's systems.
- Unless the information system is unavailable for maintenance or there is a specified business reason preventing routine User Access, TAP users may not deliberately deny authorized Users Access to systems. Back to Table of Contents

Workstation Security - Workstation Locking

All workstations used to access eSI must be protected from unauthorized access. To reduce the risk of unauthorized access to protected health information, systems must be locked or logged off when not in use. To decrease the likelihood of systems being left logged on and abandoned, a network policy or application policy to terminate sessions after **30** minutes of inactivity shall be used. Systems must be physically segregated from publicly accessible spaces whenever possible. When systems must be deployed to publicly accessible spaces, they should be physically secured from theft or tampering with appropriate security mechanisms or locks. Screens are to be turned from public visibility whenever possible. When not possible, screen protectors must be used to reduce the risk of shoulder surfing. All systems used to store, process, transmit or receive protected health information must implement drive encryption.

Back to Table of Contents

Device and Media Controls - Accountability

All movement or removal hardware and electronic media that contain eSI must be tracked by the CISO/Privacy Officer including a description of the hardware or media, the information that it contains, and the responsible party. Receipt or relocation of hardware or media that contains eSI must be confirmed once it reaches its destination. Workforce members shall coordinate hardware or media removal with their manager for approval. Managers will register the hardware or media movement, and responsible party - with the CISO/Privacy Officer. Back to Table of Contents

Device and Media Controls: Data Backup and Storage Procedures

All movement of hardware, systems and electronic media that contain eSI must be successfully backed up with an approved backup strategy that has been tested and validated prior to movement. Backups should be securely stored and encrypted. Encryption keys will be managed by the CISO/Privacy Officer. The CISO/Privacy Officer will ensure appropriate delegates perform and validate the backups prior to releasing the hardware, system, or media for movement. Back to Table of Contents

Device and Media Controls - Media Re-use

The CISO/Privacy Officer (or designated representative) oversees the sanitization of all hardware or media which contain or were used to transmit, store or process eSI before it can be reused. Documentation on the hardware or media and the information it contains, as well as a certification of sanitization must accompany the media reuse log. Back to Table of Contents

Device and Media Controls: Disposal

The CISO/Privacy Officer (or designated representative) oversees the sanitization of all hardware or media which contain or were used to transmit, store or process eSI. Documentation on the hardware or media and the information it contains, as well as a certification of destruction or sanitization must accompany the final disposition log. Back to Table of Contents

Mobile Device Security

Mobile computing devices (smartphones, tablets, convertible laptops, and various other personal computing devices) are becoming an implementation standard in today's computing environment. Their size, portability, and ever- increasing functionality are making the devices desirable in replacing traditional desktop devices. However, the portability offered by these devices can also increase security exposure to individuals using the devices.

General

All mobile devices, whether owned by TAP or owned by team member, that have access to systems and applications are governed by this policy. Applications, including cloud storage software used by staff on their own personal devices are also subject to this policy. The following general procedures and protocols apply to the use of mobile devices:

- Mobile computing devices must be protected with a password required at the time the device is powered on
- Passwords must meet the requirements outlined in the Password Management section of this document
- All TAP data stored on mobile devices shall be encrypted, but efforts should be taken to avoid storing TAP data on devices and instead in TAP's Azure cloud
- Wireless encrypted security and access protocols shall be used with all wireless network connections
- Staff shall refrain from using public or unsecured network connections while using their mobile device for work
- Personal mobile computing devices that require network connectivity must conform to all TAP standards for use and configuration
- Personal devices used for work business shall be registered with the CISO/Privacy Officer and approved by the IT Department
- Unattended mobile computing devices shall be physically secured
- Mobile computing devices that access the TAP network shall have active and up-to-date anti-malware and firewall protection
- Lost and stolen devices shall have locations services enabled and the units "bricked" or wiped of all information so they are unusable until recovered or destroyed

User Device Responsibilities

The following procedures and requirements shall be followed by all users of mobile devices:

- Staff shall immediately report any lost or stolen devices
- Unauthorized access to a mobile device or company data must be immediately reported
- Mobile devices shall not be "rooted" or have unauthorized software/firmware installed
- Staff shall not load illegal content or pirated software onto any mobile device

- Only approved applications are allowed on mobile devices that connect to the TAP network
- Mobile devices and applications shall be kept up-to-date
- Operating system and application patches should be installed within 30 days of release
- Mobile devices shall have active and up-to-date anti-malware/virus protection software
- All mobile device physical storage partitions shall be encrypted
- Personal firewalls shall be installed and active where available
- Staff shall use TAP's corporate email system when sending or receiving TAP data
- Staff are responsible for ensuring all important files stored on the mobile device are backed up on a regular basis
- Mobile Device Management (MDM) will be used to enforce common security standards and configurations on devices
- Staff shall not modify configurations without express written authorization from the IT Department

Administrative Responsibilities

The CISO/Privacy Officer or their designee shall ensure:

- Specific configuration settings shall be defined for personal firewall and malware protection software to ensure that that this software is not alterable by users of mobile and/or employee-owned devices.
- Annual security training is provided to users of mobile devices.
- Periodic security reminders may be used to reinforce mobile device security procedures.
- MDM software is used to manage risk, limit security issue, and reduce costs and business risks related to mobile devices. The software shall include the ability to inventory, monitor (e.g. application installations), issue alerts (e.g. disabled passwords, categorize system software (operating systems, rooted devices), and issue various reports (e.g. installed applications, carriers).
- MDM software enforces security features such as encryption, password, bricking, and key lock on mobile devices.
- MDM software shall include the ability to distribute applications, data, and global configuration settings against groups and categories of devices.
- Regular reviews and updates of security standards and strategies used with mobile computing devices.
- Procedures and policies exist to manage requests for exemptions and deviations from this policy.

The IT Department shall implement procedures and measures to strictly limit access to sensitive data moving to and from mobile computing devices since these devices generally pose a higher-risk for incidents than non-portable devices.

Audit Controls and Management

Satisfactory examples of evidence and compliance include:

- Spot user checks for compliance with mobile device computing policies
- Readily available processes and procedures for staff use of mobile devices
- Configuration and support guidelines and procedures for mobile devices
- Communication and device logs of attached units showing appropriate management and monitoring protocols are in place
- Anecdotal and archival communications showing regular implementation of the policy

Back to Table of Contents

4: Stewards

Information Access Management

All staff who perform Participant functions directly on behalf of the Company will have access to SI as determined by their department and job description and as granted by IT.

These employees with access may use and disclose SI as required under HIPAA or other compliance rules but the SI disclosed must be limited to the minimum amount necessary to perform the job function.

Employees with access may not disclose SI unless an approved compliant authorization is in place, or the disclosure otherwise is in compliance with this Plan and the use and disclosure procedures of HIPAA or other compliance rules.

Staff members may not access either through our information systems or the participant's medical record the medical and/or demographic information for themselves, family members, friends, staff members or other individuals for personal or other non-work-related purposes, even if written or oral participant authorization has been given. If the staff member is a Participant in TAP Innovation's plans, the staff member must go through their Provider to request their own SI.

In the very rare circumstance when a staff member's job requires him/her to access and/or copy the medical information of a family member, a staff member, or other personally known individual, then he/she should immediately report the situation to his/her manager who will determine whether to assign a different staff member to complete the task involving the specific Participant.

Your access to your own SI must be based on the same procedures available to other participants not based on your job-related access to our information systems. For example, if you are waiting for a lab result or want to view a clinic note or operative report, you must either contact your physician for the information or make a written request to the CISO/Privacy Officer. You cannot access your own information; you must go through all the appropriate channels as any Participant would have to. Back to Table of Contents

Information Access Management - Access Authorization

Before access to eSI can be established for a workforce member, that workforce member must be authorized for the appropriate level of access that their position requires. Access to eSI and systems that store or process eSI requires a valid and authorized user account and password.

Workforce members are required to authenticate themselves to these systems using their unique user accounts.

Access will be authorized based on management requests and as certified by the CISO/Privacy Officer following the Workforce Security Policy. All access requests must be submitted electronically, or in writing, and retained with the authorization. Authorization must be based on job title, roles, and responsibilities.

Once authorization is granted, the CISO/Privacy Officer will provide the program manager of the system(s) to which authorization was granted, a copy of the authorization. Program manager(s) will create, disable, or modify information systems accounts based on authorizations provided by the CISO/Privacy Officer. Back to Table of Contents

Information Access Management - Access Establishment and Modification

The CISO/Privacy Officer is required to ensure appropriate review of authorizations is conducted on a regular basis but, no later than on the anniversary of the authorization. Authorizations should be validated based on workforce members' employment status, job title, duties, responsibilities and documented authorizations. Any access that does not have corresponding authorizations or are no longer valid will be immediately provided to the program manager for termination of access. Access reviews and modifications will be documented and certified by the CISO/Privacy Officer. Items to review include access to workstations, systems logon accounts, application and process access that stores, processes, or transmits eSI.

Back to Table of Contents

Person or Entity Authentication

EVALUATE AUTHENTICATION METHODS AVAILABLE

Available authentication methods, also called factors of authentication, include something you are (Biometrics) including retina, fingerprint, palm print, or other unique characteristics of a person; something you have (token devices) including smart cards and RFID badges; and something you know (pass codes) including passwords, pin numbers, or some other form of known response.

SELECT AND IMPLEMENT AUTHENTICATION OPTION

TAP has elected to implement **FACTOR (such as password, pass code, Multifactor, biometric)** authentication to validate that any person or process requesting access to eSI is the one they claim to be.

Additional requirements are outlined in the Access Controls and the Password Policy.

Back to Table of Contents

Business Associates – Contracts/BAAs

TAP will maintain proper and effective **Business Associate Agreements (BAA)** in place with all partners who create, receive, maintain, or transmit eSI with or on our behalf. Including but not limited to Business Associates, Covered Entities, and/or sub-contractors.

Business Associates shall comply with and shall cooperate and assist TAP in its compliance with, all requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and any and all future regulations, requirements and writings promulgated thereunder.

Business Associates and their corresponding contract must require said business associates notify TAP whenever "unsecured" SI is breached. Additionally, TAP is required to notify any covered entities of such a breach without any unreasonable delay and in any event within 60 days of discovery. The notice must identify each individual whose unsecured SI is breached. It should also contain the information necessary for the covered entity to satisfy its notification obligations with respect to each affected individual.

Business Associates shall provide an individual upon request with an accounting of disclosures including disclosures made for the purpose of treatment, payment or health care operations.

Business Associates shall follow the HIPAA security rule including the assignment of a CISO/Privacy Officer, develop written policies and procedures, adopt administrative, physical and technical safeguards for SI, and train its workforce on how to protect SI.

If this organization serves (or intends to serve) as a business associate, it will adhere to the terms of its business associate agreements or contracts.

All Business Associate agreements, contracts or other relationships will be documented and reviewed regularly by the CISO/Privacy Officer. Agreements shall be reviewed, and renewed annually, or terminated and retained for documentation purposes. TAP will use the attached standard business associate agreement. Any deviation or change to the Business Associate agreement must be reviewed and approved by the CISO/Privacy Officer and must provide the same assurance to protect the confidentiality, integrity and availability of SI as specified in the standard.

Business Associate Agreements (BAA) will be signed by all TAP vendors and associates that have access to SI and/or other sensitive data. These will be reviewed annually with each vendor to ensure compliance. Back to Table of Contents

Business Associate Agreements or Other Arrangements: TAP's Full Business Associate Agreement (BAA)

The Business Associate Agreement (the "Agreement"), effective **[DATE]**, is entered into by and between ***[BUSINESS ASSOCIATE]*** (the "Business Associate") and TAP***, LLC*** (the "Covered Entity"). The Covered Entity and Business Associate may be referred to as the "Party" individually or "Parties" collectively.

This Agreement sets forth the terms and conditions governing the sharing of patient health information between the Covered Entity and Business Associate.

1. Recitals

Whereas, Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, known as "the Administrative Simplification provisions," directs the Department of Health and Human Services ("HHS") to develop standards to protect the security, confidentiality, and integrity of health information; and

Whereas, pursuant to the Administrative Simplification provisions, the Secretary of Health and Human Services issued regulations modifying 45 CFR Parts 160 and 164 (the "HIPAA Privacy and Security Rule"); and

Whereas, the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), pursuant to Title XIII of Division A and Title IV of Division B, called the "Health Information Technology for Economic and Clinical Health" ("HITECH") Act, codified at 42 U.S.C. 17921-17954, provides modifications to the HIPAA Privacy and Security Rule; and

Whereas, pursuant to the HITECH Act, the Secretary of HHS has issued regulations at 45 C.F.R. Part 164, Subpart D (the "Data Breach Rule", together with the HIPAA Privacy and Security Rule and any and all regulations promulgated under the HITECH Act, the "HIPAA Rules"), and may issue additional regulations in the future to further protect the security, confidentiality, and integrity of health information; and

Whereas, the Parties wish to entered into or have entered into an arrangement whereby Business Associate will provide services to Covered Entity as outline in the Services Agreement ("Services Agreement"), and, pursuant to such arrangement, Business Associate may be considered a "business associate" of Covered Entity as defined in the HIPAA Privacy and Security Rule; and

Whereas, in connection with these services, Covered Entity may disclose to Business Associate certain Protected Health Information that is subject to protection under the HIPAA Privacy and Security Rule; and

Whereas, Business Associate is subject to the HIPAA Privacy and Security Rule and must comply with those requirements as they apply to the Covered Entity in Business Associate's performance under this Agreement; and

Whereas, both Parties agree that the HIPAA Rules require that Covered Entity receive adequate assurances that Business Associate will comply with certain obligations with reyeect to the Protected Health Information received in the course of providing services to or on behalf of the Covered Entity, and the purpose of this Agreement is to comply with the requirements of the HIPAA Rules.

Now Therefore, in consideration of the mutual promises and covenants herein, and for other good and valuable consideration, the receipt and sufficient of which is hereby acknowledged, the Parties agree as follows:

1. Definitions

Except as otherwise defined by this Agreement, any and all capitalized terms shall have the same meaning as the definitions set forth in the HIPAA Rules and the HITECH Act, as amended from time to time. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Rules and the HITECH Act, as amended, the HIPAA Rules and HITECH Act shall control.

"Breach" shall mean the unauthorized acquisition, access, use, or disclosure of personal identifying information, sensitive personal information, or SI in a manner not permitted under the Privacy Rule or applicable state law which compromises the security or privacy of the information. For the purposes of this definition, "compromises the security or privacy of the SI" means unauthorized possession, use or disclosure of personal identifying information, sensitive personal information, or SI.

"Business Associate" shall mean the entity identified above.

"Covered Entity" shall mean *TAP, LLC*.

"Designated Record Set" shall mean a group of records maintained by or for Covered Entity, as defined by the Privacy Rule, that is: (i) the medical records and billing records maintained by or for a covered health provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained b y or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about Individuals. For purposes of this definition, the term ***"record"*** means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

"Individual" shall mean the person who is the subject of the protected health information and any person who qualifies as a personal representative under 45 C.F.R. § 164.502(g).

"Personal Identifying Information" shall mean information that alone or in conjunction with other information identifies an Individual, including an Individual's: (i) name, social security number, date of birth, or government-issued identification number; (ii) mother's maiden name; (iii) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; or (iv) unique electronic identification number, address, or routing code.

"Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. parts 160 and 164, subparts A and E as they may be amended from time to time.

"Protected Health Information" or ("PHI") shall mean Individually Identifiable Health Information that is transmitted or maintained in any for or medium created or received by Business Associate from or on behalf of Covered Entity.

"Required by Law" shall mean a mandate contained in law that compels a use or disclosure of PHI and that is enforceable in a court of law.

"Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her Designee.

"Sensitive Personal Information" shall mean an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: (i) social security number; (ii) driver's license number or government-issued identification number; or (iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or information that identifies an individual and relates to: (i) the physical or mental health or condition of the individual; (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual.

1. Obligations Of Business Associate

Business Associate acknowledges that the sections of the HIPAA Rules and HITECH Act apply directly to Business Associate as they apply to Covered Entity and agrees to comply with such rules and regulations, as outlined in the sections of part 3.0 of this Agreement.

1. Use And Disclosure of PHI

Except as otherwise permitted by this Agreement or Required by Law, Business Associate shall not Use or Disclose PHI except as necessary to provide the services as described in the Services Agreement to or on behalf of Covered Entity, and shall not Use or Disclose PHI in a manner that would violate the Privacy Rule if Used or Disclosed by Covered Entity. Notwithstanding the foregoing, Business Associate may Use and Disclose PHI as necessary for the proper management and administration of Business Associate, or to carry out its legal responsibilities, provided that Business Associate shall in such cases: provide information to members of its workforce Using or Disclosing PHI regarding the confidentiality requirements of the HIPAA Rules and this Agreement; and unless such Disclosure is Required by Law, obtain reasonable assurances from the person or entity to whom the PHI is disclosed that: (i) the PHI will be held confidential and further Used and Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person or entity; and (ii) the person or entity will notify Business Associate of any instances of which it is aware in which confidentiality of the PHI has been breached.

2. Safeguards

Business Associate shall implement reasonable and appropriate administrative, physical, and technical safeguards to ensure that PHI is not Used or Disclosed in any manner inconsistent with this Agreement and to protect the confidentiality, integrity, and availability of any electronic PHI it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the Security Rule. Further, Business Associate will implement any other security requirements to the extent required by Section 17931(a) of the HITECH Act and any applicable regulations. Business Associate will ensure that any agent, including a subcontractor, to whom it provides such electronic PHI agrees to implement reasonable and appropriate safeguards to protect it.

3. Incident Reporting

Business Associate shall report, in writing, to Covered Entity any Breach, Security Incident, or Use, Disclosure, or unauthorized access of PHI that is not permitted by this Agreement within two (2) calendar days after discovery. The report shall include, at a minimum, the identification of each affected individual. The Covered Entity retains control over breach notification procedures, including risk assessment, provision of breach notification to affected patients and communications to other entities as required, such as media outlets and the Secretary ("Breach Notification Procedure"). Business Associate shall cooperate with Covered Entity in any investigation of the incident and the Breach Notification Procedure, to include a review of breach notification and other communications as requested. In addition, Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of the requirements of this Agreement, the HIPAA Rules, or the HITECH Act, or of Sensitive Personal Information or Personal Identifying Information in violation of applicable state law.

4. Data Aggregation

In the event that Business Associate works for more than one Covered Entity, Business Associate is permitted to Use PHI for data aggregation purposes only in order to analyze data for permitted health care operations, to the extent that such Use is permitted under the Privacy Rule and the Services Agreement.

5. Minimum Necessary

Business Associate and its agents or subcontractors, if any, shall request, Use and Disclose only a Limited Data Set, if practicable; if not practicable, Business Associate and its agents or subcontractors, if any, shall request, Use and Disclose only the minimum amount of PHI necessary to accomplish the purpose of the request, Use or Disclosure, unless an exception in 45 C.F.R. § 164.502(b)(2) applies; provided that, when effective, Business Associate agrees to comply with the Secretary's guidance on what constitutes minimum necessary as required by HITECH Act Section 13405.

6. Disclosure To Agents and Subcontractors

If Business Associate Discloses PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, to agents, including a subcontractor, Business Associate shall require the agent or subcontractor to agree in writing to the same or substantially similar restrictions and conditions as apply to Business Associate under this Agreement. Business Associate further expressly warrants that its agents or subcontractors will be specifically advised of, and will comply in all respects with, the terms of this Agreement.

7. Individual Rights

Business Associate agrees that if it maintains a Designated Record Set for Covered Entity that is not maintained by Covered Entity, it will permit an Individual to inspect or copy PHI about the Individual in that set as directed by Covered Entity to meet the requirements of 45

C.F.R. § 164.524, the HITECH Act, and applicable state law. Covered Entity is required to take action on such requests as soon as possible, but not later than fifteen (15) days following receipt of the request. Business Associate agrees to make reasonable efforts to assist Covered Entity in meeting this deadline. If Business Associate maintains PHI electronically, it agrees to make such PHI electronically available to the applicable Individual. If Covered Entity maintains the requested records, Covered Entity, rather than Business Associate, shall permit access according to its policies and procedures implementing the HIPAA Rules and the HITECH Act.

Business Associate agrees, if it maintains PHI in a Designated Record Set, to make amendments to PHI at the request and direction of Covered Entity pursuant to 45 C.F.R. § 164.526. If Business Associate maintains a record in a Designated Record Set that is not also maintained by Covered Entity, Business Associate agrees that it will accommodate an Individual's request to amend PHI only in conjunction with a determination by Covered Entity that the amendment is appropriate according to 45 C.F.R. § 164.526

8. Accounting Of Disclosures

Business Associate agrees to maintain documentation of the information required to provide an accounting of Disclosures of PHI in accordance with 45 C.F.R. § 164.528 and Section 17935(c) of the HITECH Act, and to make this information available to Covered Entity upon Covered Entity's request, in order to allow Covered Entity to respond to an Individual's request for an accounting of Disclosures.

9. Internal Practices, Policies, And Procedures

Except as otherwise specified herein, Business Associate shall make available its internal practices, policies, and procedures relating to the Use and Disclosure of PHI received from or on behalf of Covered Entity to the Secretary or his or her agents for the purpose of determining Covered Entity's compliance with the HIPAA Rules, or any other health oversight agency, or to Covered Entity. Records requested that are not protected by an applicable legal privilege will be made available in the time and manner specified by the Secretary, applicable health oversight agency, or Covered Entity

10. Notice Of Privacy Practices

Business Associate shall abide by the limitations of Covered Entity's Notice of which it has knowledge. Any Use or Disclosure permitted by this Agreement may be amended by changes to Covered Entity's Notice; provided, however, that the amended Notice shall not affect permitted Uses and Disclosures on which Business Associate relied prior to receiving notice of such amended Notice.

11. Withdrawal of Authorization

If the Use or Disclosure of PHI in this Agreement is based upon an Individual's specific authorization for the Use or Disclosure of his or her PHI, and the Individual revokes such authorization, the effective date of such authorization has expired, or such authorization is found to be defective in any manner that renders it invalid, Business Associate shall, if it has notice of such revocation, expiration, or invalidity, cease the Use and Disclosure of the Individual's PHI except to the extent it has relied on such Use or Disclosure, or if an exception under the Privacy Rule expressly applies.

12. Knowledge Of HIPAA

Business Associate agrees to review and understand the HIPAA Rules and HITECH Act as they apply to Business Associate, and to comply with the applicable requirements, as well as any applicable amendments thereto.

13. Remuneration And Marketing

Business Associate will not directly or indirectly receive remuneration in exchange for any PHI, subject to the exceptions contained in the HITECH Act, without a valid authorization from the applicable Individual. Business Associate will not engage in any communication which might be deemed to be "marketing" under the HITECH Act.

14. Training Of Business Associate's Employees

In accordance with state law where applicable, Business Associate shall provide a training program to its employees, who handle or access Covered Entity's PHI, regarding HIPAA / HITECH, and state law concerning PHI that is specifically tailored to Business Associate's course of business and each employee's scope of employment with Business Associate. Such training shall occur at least once every two (2) years and within sixty (60) days of hire of a new employee. Business Associate shall maintain documentation of each employee's signed verification of attendance in such training program and provide to Covered Entity upon request.

1. Term And Termination

This Agreement shall be effective as the Effective Date and shall be terminated when all PHI provided to Business Associate by Covered Entity, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity. If Business Associate, or its agents or subcontractors, if any, violates any material term of this Agreement, as determined by Covered Entity, Covered Entity may, in its discretion: (i) immediately terminate this Agreement; (ii) provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not promptly cure the breach or end the violation within a period not to exceed thirty (30) calendar days; or (iii) report this violation to the Secretary if neither termination nor cure is feasible. Covered Entity may terminate this Agreement effective immediately, if (i) Business Associate is named as a defendant in a criminal proceeding for a violation of the HIPAA Rules, HITECH Act, or other security or privacy laws or (ii) there is a finding or stipulation that the Business Associate has violated any standard or requirement of the HIPAA Rules, HITECH Act, or other security or privacy laws in any administrative or civil proceeding in which Business Associate is involved. Business Associate agrees to report the commencement of any legal action or investigation against Business Associate arising from an alleged violation of the HIPAA Rules, the HITECH Act, or any other security or privacy laws. Upon termination of this Agreement for any reason, Business Associate agrees to return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, maintained by Business Associate in any form. If Business Associate determines that the return or destruction of PHI is not feasible, Business Associate shall inform Covered Entity in writing of the reason thereof, and shall agree to extend the protections of this Agreement to such PHI and limit further Uses and Disclosures of the PHI to those purposes that make the return or destruction of the PHI not feasible for so long as Business Associate retains the PHI.

1. Standard Provisions

1. Independent Contractors

It is expressly agreed and stipulated by and between the parties hereto that Business Associate and Covered Entity are independent contractors, and neither Party shall not be deemed or construed to be an agent, servant, or employee of the other or of any affiliates within the meaning of state or common law.

2. Indemnification

To the extent permitted by law, Business Associate agrees to indemnify and hold harmless Covered Entity from and against all claims, demands, liabilities, judgments, or causes of action of any nature for any relief, elements of recovery or damages recognized by law (including, without limitation, reasonable attorneys' fees, defense costs, costs of breach notification and mitigation, regulatory investigations by the Office for Civil Rights or state regulatory agencies, and equitable relief), for any damage or loss incurred by Covered Entity arising out of, resulting from, or attributable to any acts or omissions or other conduct of Business Associate or subcontractors or agents in connection with the performance of Business Associate's duties under this Agreement, including but not limited to breach notification costs and expenses, and attorneys' fees. This indemnity shall not be construed to limit Covered Entity's rights, if any, to common law indemnity. Covered Entity retains the final right of approval of any and all communications to Individuals, including its patients, employees, media, regulators, or any other party for whom Covered Entity may be obligated to notify. Covered Entity shall have the option, at its sole discretion, to employ attorneys selected by it to defend any such action, or to provide advice regarding breach notification, the reasonable costs and expenses of which shall be the responsibility of Business Associate. Covered Entity shall provide Business Associate with timely notice of the existence of such proceedings and such information, documents, and other cooperation as reasonably necessary to assist Business Associate in establishing a defense to such action. These indemnities shall survive termination of this Agreement.

3. Rights Of Proprietary Information

Covered Entity retains any and all rights to the proprietary information, confidential information, and PHI it releases to Business Associate. Business Associate agrees that it acquires no title or rights to PHI as a result of the Services Agreement or this Agreement. The respective rights and obligations of Business Associate under Sections 3.0 and 4.0 of this Agreement shall survive the termination of this Agreement for any reason.

4. Notices

Any notices pertaining to this Agreement shall be given in writing and shall be deemed duly given when personally delivered to a Party or a Party's authorized representative as listed within this Agreement or sent by means of a reputable overnight carrier, or sent by means of certified mail, return receipt requests, postage prepaid. A notice sent by certified mail shall be deemed given on the date of receipt or refusal of receipt. All notices shall be addressed to Covered Entity: *TAP, LLC, 549 W Commerce St, #249, Dallas, TX 75208* attention to the Chief Executive Officer and the Privacy Office.

5. Amendments

If any modification to this Agreement is required by HIPAA, the HITECH Act, the HIPAA Rules, or any other federal or state law affecting this Agreement or if Covered Entity reasonably concludes that an amendment to this Agreement is needed because of a change in federal or state law or changing industry standards, Covered Entity shall notify Business Associate of such proposed modification(s) ("Legally-Required Modifications"). Such Legally Required Modifications shall be deemed accepted by Business Associate and this Agreement so amended, if Business Associate does not, within thirty (30) calendar days following the date of notice (or within such other time period as may be mandated by applicable state or federal law), deliver to Covered Entity its written rejection of such Legally-Required Modifications. If the Parties cannot agree on the effect of any such amendment or interpretation, this Agreement may be terminated upon written notice to the other Party.

6. Choice Of Law

This Agreement and the rights and obligations of the Parties hereunder shall be governed by and construed under the laws of the State in which the Covered Entity resides, without regard to applicable conflict of laws principles.

7. Regulatory REFERENCES

A citation in this Agreement to the Code of Federal Regulations shall mean the cited section as that section may be amended from time to time.

8. Assignment Of Rights and Delegation Of Duties

This Agreement is binding upon and inures to the benefit of the Parties hereto and their respective successors and permitted assigns. However, neither Party may assign any of its rights or delegate any of its obligations under this Agreement without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed. Notwithstanding any provisions to the contrary, however, Covered Entity retains the right to assign or delegate any of its rights or obligations hereunder to any of its wholly owned subsidiaries, affiliates, or successor companies. Assignments made in violation of this provision are null and void.

9. Nature Of Agreement

Nothing in this Agreement shall be construed to create (i) a partnership, joint venture, or other joint business relationship between the Parties or any of their affiliates; (ii) any fiduciary duty owed by one Party to another Party or any of its affiliates; or (iii) a relationship of employer and employee between the Parties.

10. No Waiver

Failure or delay on the part of either Party to exercise any right, power, privilege, or remedy hereunder shall not constitute a waiver thereof. No provision of this Agreement may be waived by either Party except by a writing signed by an authorized representative of the Party making the waiver.

11. Equitable Relief

Business Associate agrees that any disclosure or misappropriation of PHI by Business Associate or its agents or subcontractors, if any, in violation of this Agreement will cause Covered Entity irreparable harm, the amount of which may be difficult to ascertain. Business Associate therefore agrees that Covered Entity shall have the right to apply to a court of competent jurisdiction for specific performance and/or an order restraining and enjoining Business Associate from any such further disclosure or breach, and for such other relief as Covered Entity shall deem appropriate. Such rights are in addition to any other remedies available to Covered Entity at lay or in equity. Business Associate expressly waives the defense that a remedy in damages will be adequate, and further waives any requirement in an action for specific performance or injunction for the posting of a bond by Covered Entity.

12. Severability

The provisions of this Agreement shall be severable, and if any provision of this Agreement shall be held or declared to be illegal, invalid, or unenforceable, the remainder of this Agreement shall continue in full force and effect as though such illegal, invalid, or unenforceable provision had not been contained herein.

13. No Third-Party Beneficiaries

Nothing in this Agreement shall be considered or construed as conferring any right or benefit on a person not party to this Agreement nor imposing any obligations on either Party hereto to persons not a party to this Agreement.

14. Headings

The descriptive heading of the articles, sections, subsections, exhibits, and schedules of this Agreement are inserted for convenience only, do not constitute a part of this Agreement and shall not affect in any way the meaning or interpretation of this Agreement.

15. Entire Agreement

This Agreement, together with all the Exhibits, Riders, and Amendments, if applicable, which are fully completed and signed by authorized persons on behalf of both Parties from time-to-time while this Agreement is in effect, constitutes the entire Agreement between the Parties hereto with respect to the subject matter hereof and supersedes all previous written or oral understandings, agreements, negotiations, commitments, and any other writing and communication by or between the Parties with respect to the subject matter hereof. In the event of any inconsistences between any provisions of this Agreement in any provisions of the Exhibits, Riders, or Amendments, the provisions of this Agreement shall control.

16. Interpretation

Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Rules and the HITECH Act. In the event of an inconsistency between the provisions of this Agreement and any mandatory provisions of the HIPAA Rules, HIPAA, or the HITECH Act, as amended, the HIPAA Rules, HIPAA, or the HITECH Act shall control. Where provision of this Agreement are different from those in the HIPAA Rules, HIPAA, or HITECH Act, as amended, but are nonetheless permitted by the HIPAA Rules, HIPAA, or the HITECH Act, the provisions of this Agreement shall control.

17. Counterparts

This Agreement may be executing in a number of counterparts, each of which shall be deemed an original, but all such counterparts together shall constitute but one and the same instrument.

Back to Table of Contents

Business Associate Agreements or Other Arrangements – Reporting

See the Requirements Policy with the Full BAA Back to Table of Contents

Uses and Disclosure - Organizational Requirements

OTHER ARRANGEMENTS

1. If a business associate is required by law to perform a function or activity on behalf of TAP or to provide a service described in the definition of business associate in §160.103 to TAP, TAP may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this policy and the Business Associate Policy if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by this policy, if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.
2. TAP may omit from its other arrangements the termination authorization required by this policy, if such authorization is inconsistent with the statutory obligations of TAP or its business associate.
3. TAP may disclose only a limited data set to a business associate for the business associate to carry out a health care operations function if a data use agreement with the business associate that complies with this policy is in place.

OTHER REQUIREMENTS FOR CONTRACTS AND OTHER ARRANGEMENTS

1. The contract or other arrangement between TAP and the business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to TAP, if necessary:
   a. For the proper management and administration of the business associate; or
   b. To carry out the legal responsibilities of the business associate.
2. The contract or other arrangement between TAP and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in this policy, if:
   a. The disclosure is required by law; or
   b. The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and
   c. The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

Business associate contracts with subcontractors. The requirements of this policy apply to the contract or other arrangement required by the Privacy Rule between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between TAP and the business associate.

Back to Table of Contents

Uses and Disclosure - Whistleblowers

TAP is not considered to have violated the requirements of the Privacy Rule if a member of its workforce or a business associate discloses protected health information, provided that:

i. The workforce member or business associate believes in good faith that TAP has engaged in conduct that is unlawful or otherwise violates professional or that the services or conditions provided by TAP potentially endangers one or more patients, workers, or the public; and

ii. The disclosure is to:

   a. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct; or

   b. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in this section. Back to Table of Contents

5: Operational Steps

Configuration Management

Configuration Management ensures that Information Technology (IT) resources are inventoried and configured in compliance with IT security policies, standards, and procedures.

This policy is applicable to all departments and users of IT resources and assets.

1. **BASELINE CONFIGURATION.** The IT Department shall:

   a. Develop, document, and maintain under configuration control, a current baseline configuration of information systems.
   b. Review and update the baseline configuration of the information system every year.
   c. Review and update the baseline configuration of the information system when required as a result of new systems or solutions implemented and as an integral part of information system component installations and upgrades.
   d. Retain one previous version of baseline configurations of information systems to support rollback.

2. **CONFIGURATION CHANGE CONTROL.** The IT Department shall:

   a. Determine the types of changes to the information system that are configuration-controlled.
   b. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses.
   c. Document configuration change decisions associated with the information system.
   d. Implement approved configuration-controlled changes to the information system.
   e. Retain records of configuration-controlled changes to the information system for at least 2 years.
   f. Audit and review activities associated with configuration-controlled changes to the information system.
   g. Coordinate and provide oversight for configuration change control activities through the PMO/Implementations Department that convenes monthly.
   h. Test, validate, and document changes to the information system before implementing the changes on the operational system.

3. **SECURITY IMPACT ANALYSIS**. The IT Department shall:

   a. Analyze changes to the information system to determine potential security impacts prior to change implementation.

4. **ACCESS RESTRICTIONS FOR CHANGE**. The IT Department shall:

a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

5. **CONFIGURATION SETTINGS**. The IT Department shall:

a. Establish and document configuration settings for information technology products employed within the information system using TAP's security policies and procedures that reflect the most restrictive mode consistent with operational requirements.
b. Implement the configuration settings.
c. Identify, document, and approve any deviations from established configuration settings for TAP solutions and systems.
d. Monitor and control changes to the configuration settings in accordance with policies and procedures.

6. **LEAST FUNCTIONALITY**. The IT Department shall:

a. Configure the information system to provide only essential capabilities.
b. Review the information system quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services.
c. Disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.
d. Prevent program execution in accordance with policies regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.
e. Identify software programs not authorized to execute on information systems.
f. Employ a deny-all, allow-by-exception policy to prohibit the execution of unauthorized software programs on the information system.
g. Review and update the list of unauthorized software programs annually.

7. **INFORMATION SYSTEM COMPONENT INVENTORY**. The IT Department shall:

a. Develop and document an inventory of information system components that:
   i. Reflects the current information system accurately.
   ii. Includes all components within the authorization boundary of the information system.
   iii. Is at the level of granularity deemed necessary for tracking and reporting.
   iv. Includes information deemed necessary to achieve effective information system component accountability.
b. Review and update the information system component inventory annually.
c. Update the inventory of information system components as an integral part of component installations, removals, and information system updates.
d. Employ automated mechanisms quarterly to detect the presence of unauthorized hardware, software, and firmware components within the information system.
e. Take the following actions when unauthorized components are detected:
   i. Disable network access by such components, or

ii. Isolate the components and notifies the Chief Information Officer and system owner.

f. Verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

8. **CONFIGURATION MANAGEMENT PLAN**. IT shall develop, document, and implement a configuration management plan for the information system that:

    a. Addresses roles, responsibilities, and configuration management processes and procedures.
    b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.
    c. Defines the configuration items for the information system and places the configuration items under configuration management.
    d. Protects the configuration management plan from unauthorized disclosure and modification.

9. **SOFTWARE USAGE RESTRICTIONS**. The IT Department shall:

    a. Use software and associated documentation in accordance with contract agreements and copyright laws.
    b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.
    c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

10. **USER-INSTALLED SOFTWARE**. IT Department shall:

    a. Establish policies governing the installation of software by users.
    b. Enforce software installation policies through controlling privileged access and blocking the execution of files using policy applied by directory service and/or application whitelisting.
    c. Monitor policy compliance annually.

Back to Table of Contents

Patch Management

Regular application of vendor-issued critical security updates and patches are necessary to protect TAP's data and systems from malicious attacks and erroneous function. All electronic devices connected to the network including servers, workstations, firewalls, network switches and routers, tablets, mobile devices, and cellular devices routinely require patching for functional and secure operations.

Software is critical to the delivery of services to TAP customers and TAP users. This policy provides the basis for an ongoing and consistent system and application update policy that stresses regular security updates and patches to operating systems, firmware, productivity applications, and utilities. Regular updates are critical to maintaining a secure operational environment.

General

All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. System components and devices attached to the TAP network shall be regularly maintained by applying critical security patches within thirty (30) days after release by the vendor. Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal systems maintenance and support operating procedures.

System, Utility, and Application Patching

A regular schedule shall be developed for security patching of all TAP systems and devices. Patching shall include updates to all operating systems as well as office productivity software, data base software, third party applications (e.g. Flash, Shockwave, etc.), and mobile devices under the direct management of the IT Department.

Most vendors have automated patching procedures for their individual applications. There are a number of third-party tools to assist in the patching process and TAP should make use of appropriate management software to support this process across the many different platforms and devices the IT Department supports. The regular application of critical security patches is reviewed as part of normal change management and audit procedures.

Patching Exceptions

Patches on production systems (e.g. servers and enterprise applications) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The risk mitigation alternative selected should be determined through an outage risk to exposure comparison. The reason for any departure from the above standard and alternative protection measures taken shall be documented in writing for devices storing non-public data. Deviations from normal patch schedules shall require CISO/Privacy Officer authorization.

Security Patching Procedures

Policies and procedures shall be established and implemented for vulnerability and patch management. The process shall ensure that application, system, and network device vulnerabilities are:

- Evaluated regularly and responded to in a timely fashion
- Documented and well understood by support staff
- Automated and regularly monitored wherever possible
- Executed in a manner applicable vendor-supplied tools on a regularly communicated schedule

Applied in a timely and orderly manner based on criticality and applicability of patches and enhancements.

Audit Controls and Management

Satisfactory examples of evidence and compliance include:

- Spot user checks for compliance with mobile device computing policies
- Readily available processes and procedures for staff use of mobile devices
- Configuration and support guidelines and procedures for mobile devices
- Communication and device logs of attached units showing appropriate management and monitoring protocols are in place
- Anecdotal and archival communications showing regular implementation of the policy

Back to Table of Contents

Vulnerability Management

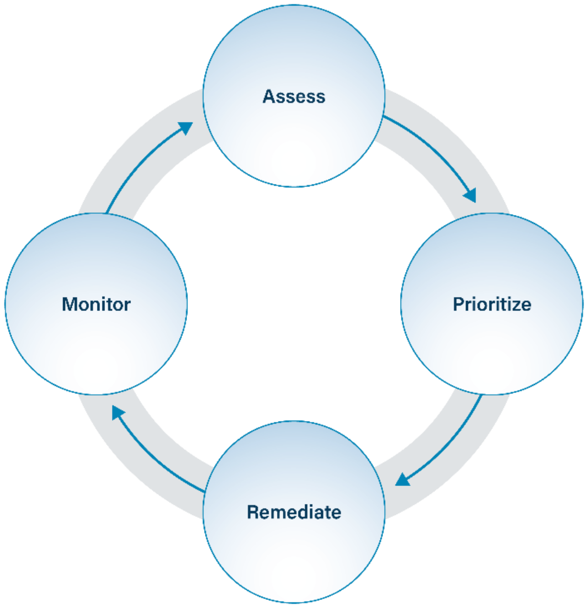
Cybersecurity professionals are constantly challenged by attackers actively searching for vulnerabilities within enterprise infrastructure to exploit and gain access. Defenders must leverage timely threat information available to them about software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Types of Vulnerabilities

There are many types of enterprise assets that may contain vulnerabilities. Assets are defined as all end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers, in virtual, cloud-based, and physical environments. Essentially any device owned, or system used by, an organization. Vulnerabilities may exist in all of these assets. All enterprise assets will contain vulnerabilities at some point in their lifecycle.

Vulnerability Life Cycle

This vulnerability management policy is divided into multiple sections based on usage patterns of assets within an enterprise. These sections are shown below in Figure 2 are the high-level "steps" of the *Vulnerability Management Lifecycle*, followed by a detailed description of what each step entails.



- **Assess** – A combination of automated scanning, manual analysis, and leveraging threat intelligence to ascertain if vulnerabilities exist in enterprise systems and software.

- **Prioritize** – Creating a prioritized list of vulnerabilities that should be remediated in a specific order. This may simply be identifying and fixing critical vulnerabilities first, or using a scoring system such as the Common Vulnerability Scoring System (CVSS).
- **Remediate** – Fixing or patching vulnerabilities to ensure they are removed or mitigated in some other way.
- **Monitor** – Ensuring that remediated vulnerabilities are no longer affecting systems or did not introduce more problems that must be solved.

The IT Department is responsible for all vulnerability management functions. Specifically, administrators are responsible for assessment and application of patching. Necessary vulnerability information must be relayed to other business units within the enterprise such as finance, accounting, and cybersecurity as required or needed. IT is responsible for informing all users of their responsibilities in the use of any assets assigned to them, such as applying updates in a regular manner or restarting their systems.

Assess

Enterprises that do not assess their infrastructure for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their enterprise assets compromised. A large number of vulnerability scanning tools are available to evaluate the security configuration of enterprise assets. Some enterprises have also found commercial services using remotely managed scanning appliances to be effective. Finally, threat intelligence sources often provide email lists, blogs, open-source intelligence (OSINT), or other data sources to alert companies about vulnerabilities in products. To help standardize the definitions of discovered vulnerabilities across an enterprise, it is preferable to use vulnerability scanning tools that map vulnerabilities to industry-recognized vulnerability rating, configuration, and classification schemes/languages described in the Further Discussion portion of this document.

In order to approach vulnerability management from a holistic perspective, it is necessary to have a written plan in place. A vulnerability management plan must be developed and maintained. This plan should detail scanning strategies, vulnerability prioritization, and remediation (to include patch management). Roles and responsibilities for various departments and positions should be detailed to ensure all employees understand their role in the vulnerability management process.

Tasks:

1. A process for performing vulnerability management must be established.
   a. This process must be documented and approved.
   b. At a minimum, the vulnerability management process must be reviewed on an annual basis or following significant changes within the enterprise.
   c. IT must monitor vulnerability announcements and emerging threats applicable to enterprise asset inventory.
   d. All systems connected to the enterprise network must be scanned for vulnerabilities.

Prioritize

Once vulnerabilities are identified, they must be fixed, or remediated. But in what order? Effective enterprises link their vulnerability scanners with problem-ticketing systems that track and report progress on fixing vulnerabilities. This can help highlight unmitigated critical vulnerabilities to senior management to ensure they are resolved. Enterprises can also track how long it took to remediate a vulnerability, after identified, or a patch has been issued. These can support internal or industry compliance requirements. Some mature enterprises will go over these reports in IT security steering committee meetings, which bring leaders from IT and the business together to prioritize remediation efforts based on business impact.

In selecting which vulnerabilities to fix, or patches to apply, an enterprise should augment CVSS with data concerning the likelihood of a threat actor using a vulnerability, or potential impact of an exploit to the enterprise. Information on the likelihood of exploitation should also be periodically updated based on the most current threat information. For example, the release of a new exploit, or new intelligence relating to exploitation of the vulnerability, should change the priority through which the vulnerability should be considered for patching. Various commercial systems are available to allow an enterprise to automate and maintain this process in a scalable manner.

Task:

1. Identified vulnerabilities must be prioritized, with more critical vulnerabilities addressed first.

Remediate

Security patches are updates to a computer’s operating system (OS) or installed software applications and are a basic part of Information Technology (IT) maintenance. The patches that developers provide often contain new features, but also contain fixes to recently discovered security vulnerabilities. Over time, operating systems go “stale” and need to be updated. Without a constant stream of security patches, computer systems can be infected by malware that can read or modify sensitive company data, or simply destroy it. Accordingly, patching operating systems and applications is one of the primary ways an enterprise can protect itself from attackers. Patching can be performed with patching tools or be configured in the operating system of a device. Patching tools may or may not be distinct tools for scanning for vulnerabilities. Assessing your patching status on a regular basis is important and many would say that the entire point of vulnerability scans is to test the effectiveness of your patch management efforts.

Some operating systems can help to remind users to update certain applications, especially those obtained within the application marketplace that is part of the operating system. With today’s platforms, app stores are not just on mobile devices. Microsoft® Windows® 10 has an app store called Windows Apps and Apple’s® store is called the MacApp® Store. Both stores can be configured to automatically install software updates from the application developer that were initially installed via an app store. Software obtained outside of an app store must be updated in an entirely different manner. Third-party software distributed outside the app store requires dedicated management software to patch it. In the end, keeping the total number of programs installed on a computer to the smallest number possible, helps with both management and security by reducing attack surface.

Tasks:

1. A process for remediating identified vulnerabilities must be established.
   - i. This process must be documented and approved.
   - ii. At a minimum, this process must be reviewed on an annual basis or following significant changes within the enterprise.
   - iii. Vulnerabilities that cannot be remediated must be submitted through the vulnerability exception process.
2. Operating systems must be configured to automatically update, unless an alternative approved patching process is used.
3. Applications must be configured to automatically update, unless an alternative approved patching process is used.
4. All users of enterprise assets have a duty to install updates for business systems and applications in a timely manner.
5. All users must ensure required reboots occur within a reasonable timeframe to ensure updates are properly installed.
6. High severity vulnerabilities must be addressed as a matter of priority

Monitor

A quality assurance process needs to exist to verify that patches and updates are implemented correctly and across all relevant enterprise assets. Monitoring should ensure that patches correctly fixed identified issues and affected assets no longer require further service. This will likely include the continuous process of re-evaluating assets that have already completed the vulnerability management process, which then leads back to the asset assessment process. As this occurs, data can be collected, stored, and analyzed that can further identify vulnerabilities through Security Information and Event Management (SIEM) systems and other technology.

Tasks:

1. IT should subscribe to a threat information service to receive notifications of recently released patches and other software updates.
2. IT must notify the decision-making authority if vulnerabilities are not mitigated in a timely manner.
3. Every month, IT must create a report containing the status of all known vulnerabilities within the enterprise.

Back to Table of Contents

6: Breach/Incidents

Security Incident Procedures

It is the responsibility of all workforce members to adhere to promptly report information security incidents and breaches. Security incidents include, but are not limited to the following events:

1. Moderate Risk
    a. Loss of a written password or sharing of passwords
    b. Failure to log off or leaving a system unattended
    c. Installation of unauthorized software

2. High Risk
    a. appropriate use of the internet or email
    b. Theft or loss of software, assets, or information
    c. Unfriendly employee termination
    d. Unauthorized access to eSI
    e. Unscheduled system downtime

3. Severe Risk
    a. Discovery or suspicion of a strange process, an intruder logging in, or attempting penetration into networks
    b. Suspicion or evidence of a virus, such as dramatic degradation of system performance
    c. Falsification, unauthorized use, disclosure, or illegal reproduction of eSI

Security incidents shall be reported as follows:

1. If an immediate threat is identified, the CISO/Privacy Officer shall be notified
2. All security incidents shall be immediately reported to the IT Help Desk
3. Review and assessment reports shall be issued to responsible management as appropriate.

Reporting and Escalation

a. Reported incidents shall immediately be classified by the Help Desk as a Moderate, High or Severe incident
b. An IT service ticket shall immediately be opened by the Help Desk to track the reported incident and the incident is to be logged in the incident log
c. The Help Desk shall immediately contact the CISO/Privacy Officer upon receipt of security incident reports
d. The CISO/Privacy Officer shall assign responsibility for investigation and resolution of each security incident to the appropriate individuals who can include, but are not limited to departmental managers, HR department, data center managers, system

administrators, applications analysts, network engineers, and network security engineer
Back to Table of Contents

Security Incident Procedures - Response and Reporting

Security incidents and breaches suspected to have been caused by workforce members shall be investigated by the CISO/Privacy Officer and the appropriate HR Director. Theft of software, assets or information shall be processed through the HR department, executive team, and law enforcement. Recording and tracking of these incidents shall be conducted by the CISO/Privacy Officer and IT service ticket(s) shall be utilized to track tasks and accomplishments.

The CISO/Privacy Officer shall adhere to the following guidelines while investigating and resolving security incidents for reporting and accountability:

1. Maintain updates on investigation and resolution progress with the IT ticket tracking system
2. Information shall be logged into a secure folder that can only be accessed by the CISO/Privacy Officer and/or other authorized individuals
3. Follow designated IT operational and audit procedures for problem resolution and system recovery
4. As necessary and applicable, inform appropriate managers and support staff of progress and research
5. Release of information, other than to authorized individuals, shall be handled through the CISO/Privacy Officer

The following define severity levels to which IT security incidents shall be assigned based on their potential impact to information and systems:

Level 1: Least severe and shall be investigated and resolved within two working days after the event occurs

Level 2: More serious and must be investigated and resolved the same day the event occurs, usually within two to four hours of the event, and must be escalated to the CISO/Privacy Officer immediately

Level 3: The most serious, have the potential to harm information and systems, and must be escalated and resolved by the CISO/Privacy Officer immediately

Review and Analysis:

B. Upon security incident resolution, a focused review shall be completed by the CISO/Privacy Officer
   1. Level 2 and Level 3 incidents shall be further reported by the CISO/Privacy Officer to the Chief Information Officer

2. All incidents shall be carefully assessed to determine that appropriate actions and necessary reporting requirements were met during the handling of the incident

C. The incident review shall also identify potential impacts, predict effects of operational changes, suggest mitigating alternative courses of action, and identify any concerns

D. Any operational changes planned or implemented so as to provide a greater level of security shall be documented and approved by the CISO/Privacy Officer

Responsibilities:

The CISO/Privacy Officer shall be responsible to take a lead role in the response to all security incidents, to ensure compliance with this policy, and, to maintain all records of incident reports, investigations, and resolutions Legal Counsel shall coordinate all communications related to external law enforcement and criminal prosecutions.

[Back to Table of Contents]

Definition Of Breach – Exceptions

1. Breach excludes:
   1. Any unintentional acquisition, access, or use of SI by a workforce member or person acting under the authority of TAP or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the privacy rule.
   2. Any inadvertent disclosure by a person who is authorized to access SI at TAP or business associate to another person authorized to access SI at TAP or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
   3. A disclosure of SI where TAP or a business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2. Except as provided above, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule is presumed to be a breach unless TAP or a business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
   1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
   2. The unauthorized person who used the protected health information or to whom the disclosure was made.
   3. Whether the protected health information was actually acquired or viewed; and
   4. The extent to which the risk to the protected health information has been mitigated.

Unsecured eSI means eSI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology.

Back to Table of Contents

Notification by a Business Associate

A business associate shall, following the discovery of a breach of unsecured eSI, notify TAP of such breach. A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).

a. Except as provided by requests for delay by law enforcement, a business associate shall provide the notification required without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
b. The notification shall include, to the extent possible, the identification of each individual whose unsecured eSI has been or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. A business associate shall provide TAP with any other available information that TAP is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available.

Back to Table of Contents

Law Enforcement Delay

If a law enforcement official states to TAP or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, TAP or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

Back to Table of Contents

Burden of Proof

In the event of a use or disclosure in violation of The Privacy Rule, TAP or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this policy or that the use or disclosure did not constitute a breach.

Back to Table of Contents

7-8: Disaster Recovery and Business Continuity

Contingency Plan

TAP will back up its computer systems regularly. If an emergency or other occurrence damage operational systems, hardware, or software that contain eSI, the practice would move operations to a reliable server/computer and restore the system to its last operational state. If the business location is damaged or unable to support operations, an alternate or temporary location will be selected until the site is restored to operational status. Reference TAP's Disaster Recovery and Business Continuity (DRBC) Plan. Back to Table of Contents

Contingency Plan - Data Backup Plan

TAP will ensure all cloud based and SaaS (Software as a Service) providers of systems used to store, process, or transmit eSI also provide disaster recovery and SLAs (Service Level Agreements) for the restoration of lost, damaged, corrupt, or compromised information or instances of the system(s), software, and information they are hosting or providing.

TAP will implement for all locally managed or on-premises systems that store, process or transmit eSI. TAP will ensure retrievable exact copies of eSI is backed up every **1** day. In the event of a disaster, backed up data will be restored to the damaged system (or a replacement system/site if the original system or site is no longer operable). Backup information will be stored on encrypted media and secured from unauthorized access, theft or tampering. Backup information will be securely replicated or transported to a geographically disparate location to protect the business from regional destruction caused by natural disasters or other events. Back to Table of Contents

Contingency Plan - Disaster Recovery Plan

To ensure that TAP can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing eSI, TAP shall establish and implement or follow a covered entity's DRBC Plan pursuant to which it can restore or recover any loss of eSI and the systems needed to make that eSI available in a timely manner.

The DRBC Plan will apply to all systems that contain eSI that TAP has operational control of. Back to Table of Contents

Contingency Plan - Emergency Mode Operation Plan

In the event of an emergency, the CISO/Privacy Officer would contact the IT professionals immediately to begin working on the ability to access and restore the data and provide secure access to critical business application(s). The CISO/Privacy Officer would contact Office Managers so staff members can be redirected to another location to begin operations. The users would continue to operate the system from an alternate or temporary location until the emergency situation is remedied. Back to Table of Contents

Contingency Plan - Testing and Revision Procedure

The contingency plan will be tested and revised (as necessary) every **12** months. The CISO/Privacy Officer will oversee all contingency plan tests with involvement from business stake holders and executive leadership. Results will be reported to leadership, and recommended revisions or changes (if required). Back to Table of Contents

Contingency Plan - Critical Applications

A critical analysis shall at a minimum include:

- An inventory of all information systems and data within those systems
- Network architecture diagrams and system flowcharts that show current structure, equipment addresses, and system interdependencies
- Identification and analysis of critical business processes related to eSI
- Identification and analysis of key applications and systems used to support critical business processes
- Documentation of the impact on patient service and business processes if specific information systems are unavailable for different periods of time (e.g. one hour, one day)
- Definition of maximum time periods that information systems can be unavailable
- A methodology for defining the criticality of information systems based on impact on patient service and business processes
- Prioritization of information systems according to their criticality and TAP Innovation's ability to function if they are unavailable
- Prioritization of data according to their criticality and time required for restoration
- The critical analysis must be conducted with significant involvement from the administrators, users and owners of information systems and processes.

The critical analysis must be conducted at least annually and may be performed internally or by a qualified third party.

Results of the critical analysis must be documented and securely maintained.

Back to Table of Contents

9: Ongoing Training, Testing, Evaluation, Audit & Adjustments

Security Awareness and Training

It is TAP's policy to train all members of its workforce, including management, who have access to eSI on its privacy and security policies and procedures. All staff members receive Security Program training. Whenever a privacy incident has occurred, the CISO/Privacy Officer in collaboration with management will evaluate the occurrence to determine whether additional staff training is in order. Depending upon the situation, the CISO/Privacy Officer may determine that all staff should receive training that is specific to the privacy incident. The CISO/Privacy Officer will review any privacy training developed as part of a privacy incident resolution to ensure the materials adequately address the circumstances regarding the privacy incident and reinforce the TAP Innovation privacy policies and procedures.

All new members of the workforce are required to complete the security awareness and training program within 90 days of their hire or contract date. The security awareness and training program will be provided by a review of policies and procedures and regularly occurring classes provided within the members' first 90 days and no later than every anniversary of their hire or contract date. Changes in information systems will be communicated to all workforce members and training provided.

This training will include training on the Breach Notification Rule.

Training - including content, delivery method, and attendees will be documented and retained by the CISO/Privacy Officer. Back to Table of Contents

Security Awareness and Training - Security Reminders

TAP will provide periodic security reminders and updates. Reminders will be sent quarterly, providing reminders of policy, best practices, current events, and/or relevant changes to policy, legislation, state, or federal law that directly affects business operations or the confidentiality, integrity, and availability of eSI.

Security reminders will be provided to all workforce members, including management. Security Reminders will be provided via email notifications and augmented with newsletters and posting at office locations. Notifications will be documented in the business-training log. Back to Table of Contents

Security Awareness and Training - Log-in Monitoring

TAP shall train its workforce members on monitoring login attempts and reporting discrepancies that the workforce member becomes aware of. Workforce members should expect that all activity on systems that store, process, or transmit eSI will be logged and recorded. In addition, all changes made to eSI will be logged and recorded.

System accounts will be locked or disabled after **3** failed login attempts. If a workforce member's account becomes locked out, they must request the account be unlocked and provide additional information to determine if the account was locked out due to member error - or suspicious activity. Any account locked or disabled by unknown or suspicious activity must be reported to information services for further investigation. Back to Table of Contents

Security Awareness and Training - Protection from Malicious Software

Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of, or access to, any business computer, network, or information.

When a virus is initially suspected the user must contact their manager and/or information services and not attempt to test for or remove the suspected Virus.

If authorized by information services, the user may execute actions needed to remove the Virus from the infected system.

Users are required to exercise caution when handling incoming Data, such as email and file attachments, and should not visit websites that are unfamiliar or have a high probability of containing Malicious Code, such as websites that offer free screen saver downloads, or free electronic greeting cards. Do not open attachments sent from people you do not know.

Do not open attachments unless you are expecting them. Some Viruses use the address book of the infected PC, so even an email "sent" from a person you know may actually be a Virus.

When sending email with attachments, provide identifying information.

Some Malicious Code uses the address book of the infected PC or server. Include some specific information in the body of the email to indicate that it is sent from you on purpose.

As a best practice, do not use generic email text, such as "Here's the file you requested". Spreaders of Malicious Code often include this phrase in an email message to make the recipient think it is legitimate. As a best practice, do use specific email text, such as "Here's the file with pricing information for product XYZ".

Users should not download software from the Internet or any other systems outside of TAP without approval from Information Services. The software including screen savers may contain Malicious Code and negatively impact the performance of existing systems or the network.

Approved Virus Checking Programs Required on all systems that connect to TAP information resources. Virus Checking Programs approved by the Information Services Department must be continuously enabled on all network connected devices. Intentionally disabling or removing Virus Checking Programs is forbidden. The frequency of the updates must not be altered by the user. Virus Checking Programs automatically update their Databases to protect against new threats. Every Virus that is discovered but not automatically removed by Virus Checking Programs must be reported to information services. Back to Table of Contents

Security Awareness and Training - Password Management

General Password Construction and Use:

The intent is to provide general password construction for users. The length of passwords should always be checked automatically at the time that users construct or select them, where the System supports.

All passwords should have at least **10** characters for all new accounts. Systems that do not support at least **10** characters should use the maximum number of characters supported by that System or application. **All user-chosen passwords should contain at least one alphabetic and one non-alphabetic character. Non-alphabetic characters include numbers (0-7) and punctuation. User chosen passwords should not be any part of speech. For example, proper names, geographical locations, common acronyms, and slang should not be employed.** All user-chosen passwords for computers and networks must be difficult to guess. Using derivatives of User-Ids, and common character sequences such as "123456789", should not be used. Personal details such as spouse's name, license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters. Adding numbers and punctuation to dictionary words increases the complexity of the password and the amount of time it takes an unauthorized individual internal or external to crack the password.

It is recommended that users do not construct passwords, which are identical or substantially similar to passwords that they had previously used. Authorized password strength tests may be performed on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it. All users are to change their login Password at least once every **90** days if the Application or System permits.

Users are responsible for all activity performed with their personal user-IDs. Passwords must not be written down, electronically stored, or left in a place where unauthorized persons might discover them. If it is necessary to document a password, passwords are to be electronically transmitted and stored under secure encryption. The electronic repository containing the password(s) must be protected with a unique password. Passwords must never be shared or revealed to anyone else besides the authorized user. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms.

All passwords need to be promptly changed if they are suspected of being disclosed or known to have been disclosed to unauthorized parties. Users must not knowingly allow others to perform any unauthorized activity with their unique user-IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users. Back to Table of Contents

Evaluation

TAP will annually determine what technical and non-technical evaluations will be performed in response to environmental and/or operational changes affecting the security of eSI.

Each policy is reviewed in accordance with the specifications of the security compliance rules.

CONDUCT EVALUATION

The Practice's policy is to review all facets of data security, integrity, reliability, and system functionality during the annual review. The CISO/Privacy Officer will coordinate with each department to review operating procedures, policies, technical and non-technical systems as they pertain to the Security Rule and the confidentiality, integrity, and availability of eSI.

Evaluations will be conducted using a combination of physical security inspections, operational observations and technical surveys of the business environment, network, and systems.

DOCUMENT RESULTS

The results of evaluations are maintained by the CISO/Privacy Officer. The CISO/Privacy Officer will make recommendations for change to policy, procedures, and technical or non-technical facets of the business and provide a recommended remediation plan in response to the evaluation.

Management will review the evaluation report and resulting recommended remediation plan and provide appropriate approvals.

REPEAT EVALUATIONS PERIODICALLY

The CISO/Privacy Officer (or designated representative) performs an annual technical and non-technical evaluation of the procedures in this document, or anytime there are significant environmental or operational changes affecting the security of eSI.

Back to Table of Contents

Audit Controls

Many computer Applications and System platforms have technical auditing capability built in. This functionality must be enabled so that User and system activity can be electronically recorded to a central Audit Log file.

Some Applications or Systems do not capture the User and System activity to a central audit log file. In this case, when the Application or System contains SI or Confidential information, the Data Owner, System or Application Administrator is responsible for manually reviewing the individual files that capture the User and System activity. This will help maintain the integrity of the Data and prevent misuse of Access Privileges.

Computer Applications and System platforms that currently don't have any technical auditing capability, the System or Application administrator should do, but is not limited to, the following:

Request the vendor add the functionality to the Application; Identify an alternative Application that provides the technical auditing functionality if financially cost effective; or Implement cost effective safeguards to further minimize unauthorized access or misuse.

Access Audits:

The Audit Logs, at a minimum, should capture information relevant to the risks that are presented to specific systems which store or access eSI or are accessible from outside the perimeter defense shall have intrusion detection and/or prevention and log intrusion attempts. Additional information which should be logged on all systems include:

- Startup and shutdown
- Access control events
- Each login, logout action and duration of access
- Access, modification, or attempted Access or modification to computer files, programs, directories, or peripherals
- Date and time the computer files, programs, directories, or peripherals were accessed

Audit Logs Review and Retention:

Persons responsible for reviewing Audit Logs should, at a minimum, review the logs for:

- Unauthorized Access attempts, or misuse of Access privileges.
- Malicious activity (e.g. unauthorized processes or services are running on the Application or System and sending information collected to an unauthorized System)
- The installation of and or execution of unauthorized programs
- Verification that security safeguards implemented are functioning as intended

The frequency of the Audit Logs review is determined by the following:

- For System and Applications that are available via the Internet or Intranet, Audit Logs should be reviewed at least weekly
- For Systems and Applications that contain SI or Confidential information that can only be accessed internally by Workforce members, Audit Logs should be reviewed at least monthly
- For other Systems and Applications, Audit Logs should be reviewed at least quarterly
- For online availability, Audit Logs should be retained for a minimum of thirty days
- If retaining the logs for a minimum of thirty days would impact System performance, the logs should be retained for the maximum amount of time that would not impact System performance
- Logs should be reviewed before they are truncated or deleted
- For offline availability, Audit Logs should be archived for at least one year

Reporting and Investigation:

Users should report any anomalies in System performance to their supervisor, System Administrator, or Application Administrator.

Reports received should be reviewed for indication of unauthorized Access or misuse.

Security concerns identified during the review of the Audit Logs should be reported to the Entity or CISO/Privacy Officer or Information Security Department Able Groups. The CISO/Privacy Officer will manage and report the investigations according to the requirements established in the Computer Security Incident Response policy.

For the purpose of performing an audit investigation and for the duration of the investigation, the CISO/Privacy Officer may request, and should be granted, Access that may include:

- User level or System level Access to any computing or communications device
- Access to information that may be produced, transmitted, or stored on equipment or premises
- Access to work areas
- Access required interactively monitoring and log System activity

It is the responsibility of each System or Application administrator to implement the audit requirements and document that the audits have been accomplished, and upon request, provide documentation to the ISO.

Back to Table of Contents

Documentation - Policies and Procedures

TAP will maintain written policies and procedures (which may include electronic form) including all action, activity or assessments which are required to be documented. Back to Table of Contents

Documentation - Time Limit

Documents will be retained for a period of 6 years from the date creation or the date when it was last in effect, whichever is later. Back to Table of Contents

Documentation – Availability

Documentation is available to all persons responsible for implementing the procedures to which the documentation pertains. Back to Table of Contents

Documentation – Updates

Documentation will be reviewed every 12 months, and updated as necessary, in response to environmental or operational changes affecting the security of eSI. Back to Table of Contents

Compliance

Team Members who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

Policy Exceptions

Requests for exceptions to this policy shall be reviewed by the CISO/Privacy Officer and/or the Chief Technology Officer (CTO). Departments requesting exceptions shall provide such requests to the CISO/Privacy Officer. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CISO/Privacy Officer shall review such requests; confer with the requesting department.

Back to Table of Contents