Attachment C

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Propio LS, LLC (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to personally identifiable: student data, student demographics, scheduling, attendance, grades, health and discipline tracking. Protected Data also includes all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts that ESBOCES and/or the participating school district has identified to Contractor in writing as sensitive or confidential data of ESBOCES and/or the participating school district. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of ESBOCES and/or participating school districts relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy provided to Contractor in advance of executing this Agreement. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall delete all of ESBOCES' and/or participating school districts' Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option, or direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, ESBOCES or the institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

<CONTRACTOR>

BY: [signature] DATED: 4/22/24

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record maintained by Eastern Suffolk BOCES.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at: http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, Or, by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract the Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;
   Answer: *The successful vendor needs to confirm that any and all data (including student, teacher, and principal data) is not to be used for any purpose, other than the encryption of that data*

2. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

   Answer: *The successful vendor will be required in the bid process to describe how they will abide by data protection and security requirements.*

3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

   Answer: *The successful vendor will be required in the bid process to describe how they will abide by data protection and security requirements at the expiration of the agreement.*

4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

   Answer: *Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:*

   Claudy Damus-Makelele, Associate Superintendent for Educational ServicesEastern Suffolk BOCES, 201 Sunrise Highway, Patchogue, NY 11772
   cdamus@esboces.org;

   Or in writing to:

   Chief Privacy Officer, New York State Education Department, 89 Washington Avenue Albany, NY 12234
   CPO@mail.nysed.gov

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

   Answer: *The successful vendor will be required in the bid process to describe how they will ensure data is encrypted and protected.*

Third Party Contractors are required to:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this ESBOCES Parents' Bill of Rights must be made a part of Contractor's Data Security and Privacy Plan.

Supplemental Information Regarding Propio As A Third-Party Contractor:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

   Propio does not use student, teacher, or principal data. However, we may inadvertently be exposed to or collect data as part of our interpreter quality monitoring process. Additionally, we may receive data if it is sent to us to be translated.

2. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

   Propio maintains rigorous data protection and security measures to safeguard sensitive data, including student and teacher information. All Propio staff are obligated to sign legally binding confidentiality agreements and data protection addendums that outline specific requirements for handling, processing, and storing sensitive data in accordance with applicable laws and standards. Propio conducts regular audits of our security measures and data handling practices to ensure adherence to these standards. Additionally, we provide comprehensive data protection training to all staff, which is regularly updated to reflect the latest security best practices and legal requirements.

   Access is restricted through stringent role-based controls to further safeguard sensitive data, and all data is encrypted in transit and at rest using industry-standard encryption methods. Propio has a robust incident response plan to quickly and effectively address a data breache or security incident should one occur, ensuring rapid mitigation and compliance with notification obligations.

3. Answer this question: When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
   Upon the expiration of the agreement, any student, teacher, or principal data will be destroyed using industry-standard methods that ensure the data is irrecoverable. If the client requires the return or transfer of data at the end of the agreement (such as a translation memory database), Propio facilitates this securely. Data is transferred over encrypted channels to ensure security during transit, and the transfer process is conducted in compliance with all applicable data protection laws to safeguard the data's integrity and confidentiality.

4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
   Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

   Claudy Damus-Makelele, Associate Superintendent for Educational Services Eastern Suffolk BOCES, 201 Sunrise Highway, Patchogue, NY 11772

cdamus@esboces.org;
Or in writing to:
Chief Privacy Officer, New York State Education Department, 89 Washington Avenue
Albany, NY 12234
CPO@mail.nysed.gov

And Eastern Suffolk BOCES may direct such inquiries to the Propio Client Success Manager.

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.
Interpretation data is stored within an AWS Virtual Private Cloud Instance located in the U.S. It is encrypted both at rest and in transit using AES256 at rest and TLS 1.2 or greater in transit, ensuring the highest level of data security.

   Translation data is stored in a Microsoft Azure database and relies on Azure Storage Service Encryption (SSE). Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant.

   Propio affirms we will:
   1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
   2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
   3. Not use educational records for any other purpose than those explicitly authorized in the contract;
   4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
   5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
   6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;

7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

Policy Title	Information Security Policies and Procedures		
Policy Number	*16-2211.2*	**Date of Last Revision:**	1/30/2023
Purpose	To establish information security safeguards and controls to secure Propio's information resources.		

1.0 Overview

Propio has adopted the policy statements and procedures outlined in this document in order to secure its *information resources*. Propio has both a legal and professional ethical obligation to secure protected health information (PHI), as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as well as personally identifiable information (PII). Propio is a business associate under HIPAA.

Propio is committed to providing the protection needed to secure confidential information from unauthorized access as well as ensuring its integrity and availability. In support of this commitment, this policy directs the philosophy and strategy for the application of information security safeguards and controls, appropriate and scalable for the size of Propio.

The scope of this policy applies to those individuals responsible for implementing information technology.

2.0 Definitions

Please reference: Appendix D for the Glossary of Terms and definitions.

3.0 Policy

Propio will implement reasonable and appropriate policies, procedures, safeguards, and controls to comply with applicable Federal and state laws regarding confidentiality and disclosure of PII and PHI and in particular, the HIPAA Security Rule standards and implementation specifications. These requirements will also be communicated to any agent or subcontractor of Propio that could possibly have access to PHI or PII.

The Information Security Officer and/or Chief Technology Officer will periodically review, update as needed, and approve changes to this policy in response to environmental or operational changes affecting security.

Information Security Policies and procedures will be reviewed and updated periodically. Original policies along with any updates of this document will be retained for six years from the date of creation or last date in effect. All policies and procedures will either be distributed to the workforce or made available on the network (fileserver, shared drive, document management system, etc.).

4.0 Procedure

Note: *The responsibilities of the workforce for information security and privacy are outlined in Workforce Policies on Privacy and Security.*

IT Security Manual

Security Policies and Procedures

Revision History

Date	Activity *(Reviewed / Updated)*	Reason	Approver
12/22/21	Final Draft	Policy Creation	Mark Dill
9/27/22	Reviewed/Updated and renumbered	Annual Policy Review	Bill Guyer

IT Security Manual

Table of Contents

1.0 Introduction 4
2.0 Responsibilities 6
3.0 Security Awareness, Training, Education 9
4.0 Risk Analysis and Management 11
5.0 Access Control 15
6.0 Remote Access 20
7.0 Security Monitoring and Auditing 21
8.0 Security Incident Reporting and Response 23
9.0 Business Continuity and Disaster Recovery Planning 24
10.0 Physical Security 25
11.0 Device and Media Controls 26
12.0 Network Security 31
13.0 Security Architecture 33
14.0 Change Control 38
15.0 Configuration Management 40
16.0 Security Evaluation 43
17.0 Exceptions for Noncompliance 45
18.0 System Life Cycle Planning 46
Appendix A – HIPAA Security Rule 49
Appendix B – Cross Reference to HIPAA Security 50
Appendix C – Information Security Officer Responsibilities 52
Appendix D – Incident Response (IR) Flowchart 53
Appendix E – Security Exception Request SAMPLE 54
Appendix F – Glossary of Terms and Definitions 55
Appendix G – Training Education and Awareness Plan 60
Appendix H – Cross Reference of the IS Security Manual to NIST Cybersecurity Framework 62
Appendix I– Cross Reference of the IS Security Manual to PCI DSS 3.2 66
Appendix J – Cross Reference of the IS Security Manual to ISO 27001:2013 67
Appendix K – Cross Reference of the IS Security Manual to CIS Top-20 69
Appendix L – Cross Reference of the IS Security Manual to HITRUST 9.1 71

1.0 Introduction

This *IT Security Manual* establishes Propio's information security policies and procedures.

Propio is committed to maintaining an environment that protects its information resources and its clients' data from accidental or intentional unauthorized use, modification, disclosure, or destruction. Adherence to the information security policies in the *IT Security Manual* ensure the confidentiality, integrity, and availability of Propio information and protects the interests of Propio, its owners, workforce, and business partners.

1. Guiding Principles

Information security is:

- A cornerstone of maintaining public trust
- Primarily a business issue – not just a technology issue
- Risk-based and cost-effective
- Aligned with Propio's priorities, industry-prudent practices, and regulatory requirements

1.1.3 Importance of Compliance

1. Maintaining Client Trust

Propio's clients entrust their patient information to Propio —information that must be protected by contractual requirements in addition to regulatory requirements.

2. Information Security, HIPAA/HITECH Act, and CCPA

HIPAA: Organizations that collect individually identifiable health information (IIHI), also known as protected health information or PHI, are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health IT for Economic and Clinical Health Act of 2009 (HITECH Act) and as amended by the Omnibus Rule.

HIPAA/HITECH requires business associates, including Propio, to adhere to reasonable and appropriate administrative, physical, and technical safeguards regarding the use and disclosure of PHI.

CCPA: The California Consumer Privacy Act (CCPA), officially called AB-375, is a state statute that went into effect on January 1, 2020. It is intended to enhance privacy rights and consumer protection for residents of California.

3. Designation of Responsibility for the Information Security Program at Propio

Brian Singer, Propio's CIO and CTO has delegated the authority for implementing the information security controls to Bill Guyer, the IT Compliance Officer. The responsibilities of the Information Security Officer are defined in Appendix C.

1.2 Procedures

1.2.1 IT Security Manual Revisions

An effective date and revision history will be used to assure that the *Information Technology (IT) Security Manual* is current. When the *IT Security Manual* is updated, the previous version must be retained for six years to comply with HIPAA's Security Rule. Changes to this manual are reviewed and approved by the ISO.

2.0 Responsibilities

This chapter outlines the various information security-related roles and responsibilities.

2.1 Policy

Information security is the individual and collective responsibility of the workforce. Security-related roles and responsibilities are identified in this section of the *IT Security Manual*. The separation of duties and responsibilities will be considered when defining roles, although that can be challenging because of the size of the staff.

2.2 Procedure

2.2.1 Privacy and Security Committee

Role: Provide strategic leadership for complying with various regulatory requirements, including those that pertain to information security and data privacy

Scope of responsibility:

- Attend and participate in scheduled, quarterly committee meetings (starting Q1, ’22)
- Review and approve organizational-wide policies, procedures, standards, and guidelines for the protection of information resources and data privacy
- Ensure compliance with policies and procedures
- Approve or deny requested exceptions to policies
- Recommend appropriate sanctions for violations
- Support efforts to expand security awareness of the workforce; approve the training strategy and content for the workforce
- Help determine the organization’s risk tolerance
- Recommend additional security safeguards and controls to enhance information security in a cost-effective manner
- Participate in security incident response and investigation of reported exposure, misuse, loss, theft of organization information or its falsification/alteration
- Assigned an official spokesperson for any requests from the news media or outside organizations, especially as it relates to an incident or a data breach
- Address security issues that cannot be resolved by others

2.2.2 Information Security Officer (ISO)

Role: Recommend appropriate security measures based upon risk; ensure policies, procedures, and standards exist for safeguarding, controlling, and monitoring information resources; accountable to the CEO and the Privacy and Security Committee

Scope of responsibility:

- Direct and oversee the information security program
- Work to enhance information security in a cost-effective manner
- Participate in the Privacy and Security Committee meetings
- Oversee the risk management program for information security, which includes risk analysis to guide the organization in developing security standards and procedures
- Assist in determining which workforce activities to audit, how audits will be conducted, and how long to retain audit information
- Lead the information security incident response team – investigate reported information security incidents

- Manage reported information security incidents and ensure the prevention, detection, containment, and correction of security incidents and privacy breaches
- Work cooperatively with the Privacy Officer to investigate, notify and manage actual, suspected, and potential breaches of electronic protected health information (PHI)
- Work with the Privacy and Security Committee to develop and maintain a training strategy for the workforce
- Send out periodic security reminders to the workforce to familiarize them with security policies, threats, and recommended practices
- Verify that information is properly classified

2.2.3 Chief Information Officer (CIO)

Role: Oversee the management of information technology hardware, system software, and data; maintain technical security controls

Scope of responsibility:

- Implement technical security controls to ensure the confidentiality, integrity, and availability of client data and information resources
- Review and approve security safeguards and controls, including standards such as encryption
- Maintain a balance between user functionality and security
- Participate in the Privacy and Security Committee meetings
- Present requests for exceptions to information security policies to the Privacy and Security Committee
- Ensure that periodic vulnerability assessments are conducted
- Review and approve data backup plans
- Review change requests and evaluate the possible risk and impact; ensure change requests for major applications or systems are evaluated in a test or development environment before implementing in the “Production” (or “Live”) environment
- Support the development of backup plans and a disaster recovery plan
- Maintain the highest level of protection over privilege accounts – unique user accounts and passwords (different from their normal “user credentials”) and multifactor authentication or by following more stringent password standards
- Monitor and control access to data through the administration of user accounts, including additions, deletions, and modification of privileges
- Design and develop applications following secure coding practices and based on industry standards and/or best practices
- Ensure functional testing and security code review are conducted
- Assess problems; troubleshoot and debug code
- Make recommendations for changes and improvements for reliability
- Create and maintain technical documentation
- Create separate environments for development/test from production
- Ensure that system components and software are protected from known vulnerabilities; install applicable vendor-supplied security patches in a timely manner
- Follow change control processes
- Incorporate information security throughout the software-development lifecycle

2.2.4 Compliance Officer

Role: Responsible for programs, policies, and practices that ensure Propio follows all applicable regulations and standards

Scope of responsibility:

- Creates well written policies and procedures to ensure compliance with applicable regulations.
- Communicates requirements to team members through policies, procedures, and training
- Encourages all team members to report any suspected compliance violations or concerns
- Monitors and audits for non-compliant behavior
- Promptly investigates any potential compliance violations
- Reports compliance violations timely
- Cooperates with any investigation of a potential violation by an outside organization
- Assures corrective action steps are implemented for any noted deficiencies and monitors corrective action
- Prepares compliance reports for senior leadership and provides training as needed.

2.2.5 Senior Leadership

Role: Protection of information assets within their areas of responsibility

Scope of responsibility:

- Authorize workforce access to information resources
- Notify the CTO to remove workforce access
- Periodically validate the access rights of the workforce to information resources
    - Applications - at least annually
    - Active Directory - annually
- Provide initial investigations of potential security incidents and report incidents to the Information Security Officer
- Develop contingency plan(s) for maintaining business operations when information resources are unavailable
- Verify workforce compliance with the workforce policies on information security
- Ensure users are trained on their information security responsibilities
- Sign risk analysis reports

3.0 Security Awareness, Training, Education

An effective awareness and training program is essential for information security. Without knowing the necessary and appropriate security measures (and understanding how to use them), the workforce cannot be truly accountable for their actions.

Propio training covers HIPAA, information security, and data privacy to ensure its workforce understands their responsibilities, company policies, and HIPAA. The workforce is required to participate in the training.

3.1 Policy

In addition to their initial training, the workforce receives annual awareness training (mandatory), a phishing simulation campaign, and periodic security reminders on information security and data privacy.

3.2 Procedure

3.2.1 Identification of Training Needs

Training is focused on the needs of the workforce and client requirements. Security awareness training is updated at least annually based upon such significant changes or events as:

- New or updated policies and procedures
- Changes in laws and industry regulations
- New technology, applications, or systems
- Recognized threats or vulnerabilities (cyber-attacks, phishing, ransomware, etc.)
- Security incidents (lessons learned)
- Changes in organizational and reporting structure

3.2.2 Training

The workforce receives training during their orientation with Propio and annually thereafter. The workforce needs to pass a quiz (skills check) along with their annual training.

The workforce participates in a phishing awareness campaign which periodically sends simulated phishing emails to corporate members and offers education if the phishing email is successful. IT and HR have access to the results of each simulation.

Additional training may be provided to meet the needs of an individual's work assignments and/or responsibilities.

Some Propio clients may also require individuals to complete their HIPAA training and sign their confidentiality agreements.

To reinforce the training, the workforce signs several contractual documents pertaining to their responsibilities for safeguarding data such as PHI and PII.

3.2.3 Periodic Security Reminders

Security reminders or awareness messages will be created and distributed to the workforce as needed by the IT Operations Leadership (as overseen by the CTO and Compliance Officer). Awareness reminders will usually be sent to the workforce by email

Awareness reminders may include:

- Accessing information only on a “need to know” basis
- Appropriate and acceptable use of technology
- Proper password management
- Techniques for avoiding malicious code (viruses, spyware, phishing, ransomware, etc.)
- User responsibilities for logging off computer systems before leaving it unattended
- Threats and risk of remote access (such as accessing unsecured wireless networks) and the required security controls to reduce risks to an acceptable level
- Instructions on how to identify and report security incidents and privacy breaches
- Proactive workforce phishing

3.2.4 Training Strategy

The ISO will work with the Privacy and Security Committee to determine the training content and delivery method. See Appendix H: Training Education and Awareness Plan

3.2.5 Proof of Compliance – Retention

Educational materials and security reminders are retained for six years as proof of compliance with HIPAA.

4.0 Risk Analysis and Management

Risk analysis is the process of identifying vulnerabilities or weaknesses of a system and assessing the possible damage that could be caused if those vulnerabilities or weaknesses were successfully exploited. The HIPAA Security Rule requires a risk analysis.

Risk management is the implementation of security safeguards and controls to reduce risk to an acceptable level and maintain that level of risk.

4.1 Policy

Propio will conduct risk analysis on an annual basis in conjunction with its risk management process or when:

- There are significant changes to the information technology infrastructure, application environment, or operational changes
- Newly discovered vulnerabilities or risks
- Security incidents reveal weaknesses that need to be addressed

Once risks are identified, Propio will document the Privacy and Security Committee's decisions to either implement security measures that reduce the risks to an acceptable level, accept the risk, or in some cases, insure against or transfer the risk.

Risk analysis follows the process outlined in Figure 4.1.

4.2 Procedure

4.2.1 Risk Analysis

The risk analysis process is based on the following nine steps:

1. **System Characterization**. Maintain an inventory of information resources and the security measures protecting those systems.
2. **Threat Identification**. Identify reasonably anticipated threats to information resources. Such threats may be natural, human, or environmental.
3. **Control Assessment**. Assess the security measures that have been implemented or will be implemented to mitigate identified vulnerabilities.
4. **Vulnerability Identification**. Identify known vulnerabilities of information resources. This is completed by regularly reviewing vulnerability sources and by performing security assessments. Please see section 4.2.7, *Vulnerability Scanning and Penetration Testing*.
5. **Likelihood Determination**. Assign ratings that indicate the probability that a vulnerability will be exploited by a particular threat. Three factors to consider are:
    - Threat motivation and capability
    - Type of vulnerability
    - Existence and effectiveness of current security controls
6. **Impact Analysis**. Determine the impact that would result if a threat were to successfully exploit a vulnerability of an information resource.

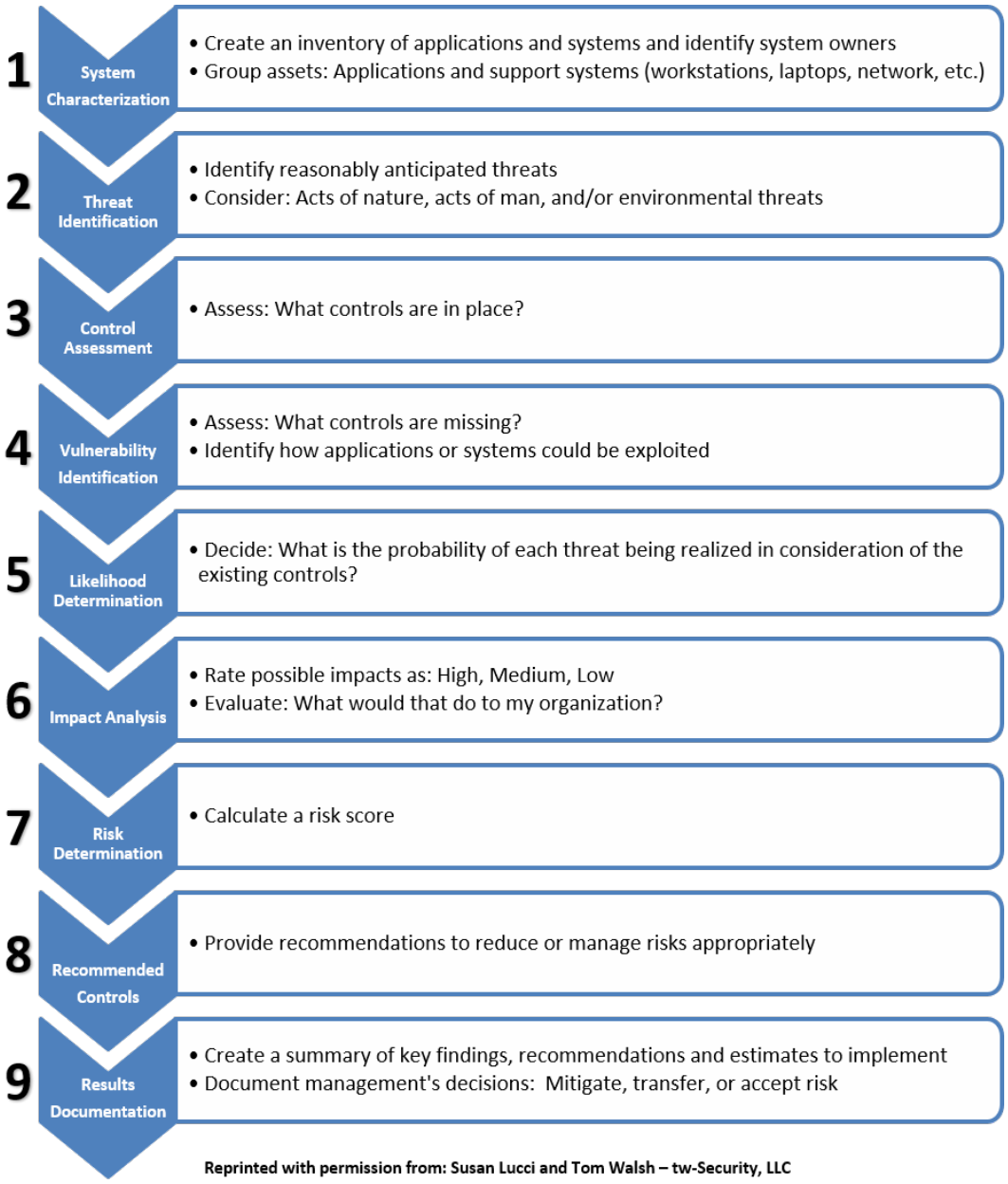
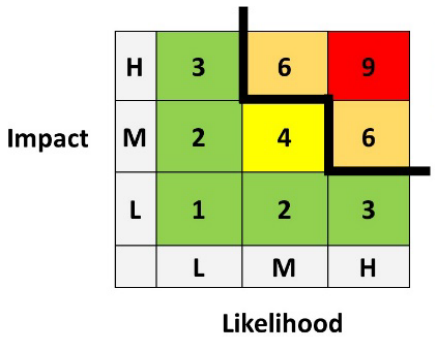


Figure 4.1 – The Risk Analysis Methodology Flowchart

7. **Risk Determination**. Use the information obtained in the previous six steps to identify the overall level of risk to specific information resources. For each vulnerability and associated possible threat, Propio will rank the risk on a scale from high to low based on the:
    - Likelihood a certain threat will attempt to exploit a specific vulnerability
    - Level of impact should the threat successfully exploit the vulnerability
    - Adequacy of planned or existing security controls

    The sensitivity of the information stored and processed is also a factor. Risks are scored using the OCTAVE approach.



Risk Management Strategy	
Score	Strategy
6-9	Must Manage Risk
4	Should Manage Risk
1-3	May Consider Managing Risk

Figure 4.2 – The OCTAVE Approach for Determining Risk Score

8. **Control Recommendations.** Additional controls are recommended to further reduce the identified risks. When deciding what resources should be allocated to mitigate identified risks, the highest priority will be given to those risks with the highest risk rankings.
9. **Results Documentation.** A risk analysis report will be created. The report will identify risks that warrant management's attention by listing:
    - Findings – Weaknesses (vulnerabilities)
    - Recommendations – Includes cost-effective safeguards and controls
    - Estimated resources – To implement the recommendations

4.2.2 Risk Profiles

Risk profiles are created to document the reasonably anticipated threats, existing security controls, vulnerabilities and the associated risks. The risk profiles streamline future risk analysis by providing a starting point, which only needs to be reviewed for changes.

4.2.3 Risk Analysis Reports

The Privacy and Security Committee will review the risk analysis report and decide how the risks will be handled. There are two choices (Y/N) regarding the recommendations for additional safeguards and controls:

- **Y = Implement** the suggested recommendation to mitigate or reduce risks to an acceptable level or look for a different solution to reduce risks;
- **N = Accept** the risk for now and continue operating the information system in its current configuration and not implement the recommendations.

If a risk is accepted (no – the suggested recommendation will not be implemented) – then a rationale for why the risk is accepted should also be listed on the report.

The CTO will sign the risk analysis report as an acknowledgement of the corrective action and/or acceptance of residual risks.

4.2.4 Risk Management/Risk Remediation Plans

Risk remediation plans are created to assure follow through for any decision to implement a safeguard or control or to transfer or insure against a risk. The plan is used to assign responsibilities, follow up on risk remediation activities (start and completion dates) and document comments, especially when obstacles are encountered

4.2.5 Updates

At a minimum, risk profiles are reviewed at least annually, when significant changes occur to the computing environment, or when new threats or vulnerabilities are discovered. Significant changes include but are not limited to:

- Security incidents
- Significant changes to the organizational or technical infrastructure
- Significant changes to an information resource or security responsibilities
- Newly discovered threats or vulnerabilities

4.2.6 Document Handling and Retention

Because the risk analysis report and the risk profiles document the vulnerabilities within an information system, these documents are considered **confidential** information and need to be protected in accordance with organizational policy.

These documents also provide proof of compliance with the HIPAA Security Rule and therefore must be retained for six years.

4.2.7 Vulnerability Scanning and Penetration Testing

Quarterly vulnerability scanning is conducted by internal staff. Any significant (critical or high) vulnerabilities identified by the scans will be addressed by the CTO. Please see Chapter 16, section 16.2.2, *Evaluation – Technical*.

Annually, a qualified security vendor, consultant, or qualified staff member will be used by Propio to perform an external penetration test and as needed, an internal penetration test to identify vulnerabilities that could be potentially exploited by an attacker to gain access to the Propio Software. **Note:** A vulnerability assessment is expected to be completed by the Pen Tester.

5.0 Access Control

Access control pertains to the logical access to information resources and electronic media. While the workforce needs access to information to do their jobs, it is important to control the level of access to the minimum necessary (such as the ability for the average user to run, but not change, system programs). These access restrictions help protect the confidentiality, integrity, and availability of data. Access controls ensure compliance with the "minimum necessary" in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.

5.1 Policy

Access to information resources is limited to authorized workforce members, support staff, and software programs (such as batch processes) that have a legitimate business need. Authorized access privileges are based upon an individual's role and responsibilities. Security controls are implemented to prevent unauthorized individuals from obtaining access to information resources.

Access to applications that contain confidential information will be based on unique user identifiers, enabling Propio to track application and system activities back to an individual or entity through audit or event logs.

5.2 Procedure

5.2.1 Authorization

Upon hire, HR and the hiring manager request access via the XenDesk ticketing tool through a process approved by the Chief Information Officer (CTO); Leadership confirms which Propio applications and systems are needed by an individual to perform their work. Access is then established based upon the lowest level of privileges needed by workers to perform their job (read or view only, create, edit, delete, etc.). Any exceptions to the normal privileges requires approval from the CTO.

Changes to an existing user's access privileges are authorized are handled in the same manner.

5.2.2 Identification of Users

Access will be based on unique user identifiers, enabling Propio to track application and system activities back to an individual or entity through audit or event logs. Technology onboarding will develop the user profile within Active Directory (AD) or the applicable application(s) or system(s) and assign each member of the workforce a unique user ID along with an initial (temporary) password.

There are two types of user IDs (accounts) in use:

- **User accounts** – for general use by the workforce for accessing computers, applications, databases, and systems.
- **Support accounts (or service accounts)** – accounts used by information technology (IT) staff and the CTO for administration of systems, applications, databases, and network devices or to automatically execute a batch process such as data backups.

If a user will also be assigned system administrator privileges, they will need different user IDs. For example:

- One user ID for their routine, work-related access
- Second user ID for conducting their system administrator duties

Generic user IDs (or shared user accounts or service accounts) are only allowed either where the functions accessible or actions carried out by the user ID do not need to be tracked, or where there are other controls in place for logging and monitoring user activities. All support accounts must be approved by the CTO at each quarterly user access review.

5.2.3 Authentication of Users

Appropriate and reasonable mechanisms are in place to ensure that only properly authenticated persons and entities access its information resources. Complex passwords are the primary method used to authenticate the workforce. Multifactor authentication (MFA) is used whenever possible.

Password and PIN-based authentication systems mask, suppress, or otherwise obscure passwords and PINs so that unauthorized persons are not able to see them. Passwords and PINs are encrypted while being transmitted between the client and the server (application/system) and at rest, whenever possible.

The first-time a user logs on to an application or system, they should be required to change their initial password(s) issued and forced to select another password; and as applicable, setup their multifactor authentication.

Applications and systems used by Propio limit the number of unsuccessful logon attempts to a maximum of 5, before locking out a user account.

5.2.4 Password Management

Passwords must be at least eight (8) characters in length and use three of the following four categories:

1) At least 1 upper case character
2) At least 1 lower case character
3) At least 1 numeric character
4) At least 1 special character (*if allowed by the system*)

In addition: Passwords privileged or elevated access (e.g., sysadmin or service account) must be at least 15 characters in length and use at least three of the following four categories as listed above.

Note: *In some cases, the application or system may not allow two different password policies: 1) user and 2) sysadmin or service account. In those cases, system administrators will create as strong of a password as possible. This will be on the honor system.*

Passwords must be changed immediately if it is believed they have been compromised.

5.2.5 Password Resets / Unlocking User Accounts

Good judgment should be exercised when validating the identity of the individual requesting that their passwords be reset or when unlocking a disabled user account.

5.2.6 Automatic Lockout (End user devices)

The workforce are required lock (via a password-protected screen saver) or shutdown the workstation whenever they plan to leave their workstations unattended for an extended period of time. This is done to prevent incidental disclosure of PHI, PII, or other confidential information.

The password-protected screen saver will activate after 15 minutes of inactivity, at a minimum. Please see Chapter 13, *Security Architecture* for additional information on workstation controls.

5.2.7 Emergency Access

This HIPAA Security Rule implementation specification is not applicable to Propio. However, in emergencies the CTO shall make the final determination of who and how authorized individuals and teams can access systems.

5.2.8 Encryption

When necessary, encryption is used to protect access to confidential information stored in the hard drives of servers, SANs, workstations, mobile devices (laptops, tablets, and smartphones) and in media (USB thumb drives, memory cards, DVDs, etc.). Encryption methodologies are reviewed and approved by the CTO. Please see Chapter 11, *Device and Media Controls* for additional information. When encryption is deemed unreasonable, the rationale for not encrypting and compensating controls used to achieve access control should be documented.

5.2.9 Access for Vendors

Propio has a responsibility to ensure that its subcontractors comply with the same terms and conditions that Propio must comply with in a business associate agreement (BAA) or some other type of contractual agreement such as a security agreement with its clients. A signed sub-BAA must be in place to govern the sharing of client's PHI with vendors.

Quarterly the IT Compliance Manager or the Director of Global IT will oversee a review of vendor access privileges to validate that access still is needed and that user privileges still are appropriate.

Please see Chapter 6, *Remote Access* for additional requirements and Propio's *Vendor Management* policy.

5.2.10 Workforce Clearance Procedure

Prior to beginning work with Propio and gaining access to PHI, the workforce will be vetted through a background investigation /clearance processes including verification of – education, references, federal crime, state crime, and/or credit checks (if Propio deems appropriate).

New workforce members will participate in an onboarding process that includes a review of the policies pertaining to PHI within 30 days of their hire date.

5.2.11 Inactive Accounts

User accounts in AD will be periodically reviewed, primarily to identify potentially overlooked terminations. After a predetermined period of inactivity for a user account (For example, 90 days), the workforce will have their information system privileges disabled. Note: Going forward, it is Propio's intent to apply this same control to non-LDAP integrated applications.

5.2.12 Terminations (Voluntary)

Access privileges are disabled or removed by the IT Ops when a user no longer needs access to information resources because of their termination.

When the workforce leave, they must return Propio property in their possession.

If a departing member of the workforce has used cryptography on Propio's data, they *must* make the cryptographic keys (passwords) available to the CTO.

The workforce will be reminded of their continuing confidentiality obligations (legal and contractual) after their contract with Propio ends.

5.2.13 Terminations (Involuntary)

Involuntary terminations follow the same procedure as voluntary except access is disabled or removed before or while the workforce member is being notified of their termination.

5.2.14 Automated Access Controls

Applications and systems may use automatic access and authentication through another trusted system such as Active Directory (AD) or through a single sign-on solution. Please see Chapter 13, *Security Architecture* for additional information.

5.2.15 Service Accounts

A service account often is a built-in (domain and/or local) administrative level account that does not correspond to an actual person and is needed to perform such automated activities or executable programs such as running batch files, backups, and system monitoring – activities that require authentication. Once established, services normally run automatically without user interaction. Sometimes service accounts require rights to the entire domain and even other domains with trust relationships. Because the passwords to service accounts are trusted and usually are not changed, these accounts are more vulnerable as targets for outside attacks.

Service accounts guidelines include:

- Create the accounts from scratch, rather than copying an existing service account, which could accidentally lead to greater privileges or access rights
- Set the service account for the appropriate permissions and access
    - Create a separate group if a service account needs to be shared, rather than placing the service account into an existing privileged group
    - Set to the minimum privileges required for the tasks performed
    - Allow a service account to only log on to certain machines

    - Use an access control list to protect sensitive files, folders, groups, or registry objects
    - Remove unnecessary rights including: “deny access to this computer from the network,” “deny logon locally,” and “deny logon as a batch job”
- Enable logging of activities associated with the service account
- Monitor the activities associated with the service account

6.0 Remote Access

A variety of controls are implemented by Propio to provide secure remote access to information resources. Propio is a hybrid/virtual company that uses cloud-based applications. Therefore, all of Propio's applications and systems are accessed remotely. Members of the workforce use secure remote connections to do their work.

6.1 Policy

The Chief Information Officer (CTO) in collaboration with the Information Security Officer (ISO) and the Privacy Officer will determine the security safeguards and controls needed for access information resources. In some cases, clients may have additional requirements for remote access to their protected health information (PHI).

Propio determines client access and remote access tools/protocols used to gain access to the Propio software.

6.2 Procedure

6.2.1 Responsibilities

The CTO will:

- Establish secure remote access to information resources
- Track vendors' with remote access
- Approve / Enable vendor access only for the time period required to accomplish previously defined contracts and/or approved tasks (whenever possible)
- Terminate remote access with vendors if it is determined that they are not meeting the security requirements set forth by Propio

6.2.2 User Remote Access (Workforce)

Propio has a list of security requirements that are reviewed with the workforce as part of their work-agreement (to be noted in the WIP Handbook, due in Q4, '21). The security requirements needed by the workforce are covered in awareness training. All remote access uses multifactor authentication.

6.2.3 Vendor Remote Access *(IT Support Vendors e.g., Microsoft)*

Direct connection requests to Propio's information resources will require secure network access and is coordinated through the CTO.

6.2.4 Vendor Responsibilities

Vendors are to comply with the following requirements:

- Preventing the alteration of any security configuration settings without Propio's approval
- Reporting any security incidents immediately to the CTO, Information Security Officer (ISO), and/or Privacy Officer
- Notifying Propio when connectivity is no longer required
- Breaking the network connection between Propio and the vendor if either site's information resources become infected with malicious code, such as a virus or ransomware that cannot be immediately removed

7.0 Security Monitoring and Auditing

Security monitoring and auditing is used to identify and resolve problems within information resources. *Monitoring* uses tools and techniques to identify security events in real-time. *Auditing* is the process of reviewing system activity records, such as audit logs to identify abnormal behavior. Audit logs can be used as *forensic* data, allowing past events to be reconstructed.

7.1 Policy

Propio conducts monitoring and auditing of its information resources as described below.

7.2 Procedure

7.2.1 Monitoring Processes

Monitoring is based on:

- The risk analysis of the information resource
- Importance of the application or system
- Value or sensitivity of the data stored within the application or system

The real-time monitoring process may include looking for:

- Faults and error states in hardware (applications, servers, network equipment, etc.)
- Anomalies in operational events
- Information system start-up or shut-down
- Failed logon attempts
- Use of such privileged accounts as system administrator accounts
- The DataDog tool is used to monitor and alert on infrastructure, application, database, network, and security activities; alerts are sent to:
    - Architect
    - Ops. Leadership
    - Agents who are on pager duty

7.2.2 Auditing Processes

Propio has established two general levels for auditing user access:

Level 1 – User access privileges

User access privileges are quarterly reviewed to validate user privileges are appropriate.

Level 2 – User activities (monitored in real time via DataDog)

Audit logs may capture and store specific data including:

- Name of affected data, system component, or information resource
- User identification (Username or user ID)
- Date and time
- Type of user activity or event (View, edit, delete, etc.)
- Origination of the user's access (IP address or MAC address)

Audits of user activities can be performed as targeted or random audits.

Targeted Audits – A targeted audit may be requested by management to the Chief Information Officer (CTO) who will then generate an audit report to review the user's

activities. The Privacy Officer needs to be involved from the start in case sanctions are necessary.

Random Audits – A random audit of user activities as determined by the Privacy Officer.

7.2.3 Responsibilities for Reviewing System Activity

The CTO and the Privacy Officer are responsible for conducting Level 1 and 2 audits. Overseen by leadership, executed by Propio's Operations staff, the IT Architect and/or on call staff.

8.0 Security Incident Reporting and Response

A *security incident* is any adverse event that threatens some aspect of computer security, including loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Incident reports can be used to facilitate future risk analysis by providing data on the probability or likelihood of an event occurring again and helping estimate the potential impact to the organization.

Prompt response to suspected or actual security incidents is a critical part of Propio's ability to safeguard its information resources and a client's protected health Information (PHI) or other sensitive information.

8.1 Security Incident Response Plan

Propio will appropriately respond to reported information security incidents following the steps outlined in this procedure, which are based upon guidelines from the National Institute of Standards and Technology (NIST). Appendix C lists a reference of the possible regulatory requirements and the NIST Cybersecurity Framework (CSF) criteria applicable to incident reporting and response.

An incident report will be created, updated, and retained as mandated by regulatory requirements. Incidents will be categorized and the appropriate response procedures will be followed based upon the severity of the incident. Post-incident activities will be used as opportunities for improvement to try and reduce the likelihood of a similar incident occurring again.

Depending on the type of incident and the data type involved, incident response procedures may also have to follow regulatory requirements as well.

In addition to this procedure, the Incident Management Plan (which is essentially the disaster recovery plan), may also be used for response guidance.

See Propio's NIST-based response procedures for more information

9.0 Business Continuity and Disaster Recovery Planning

The information resources of Propio are assets of significant value because they contain information that is an integral part of business functionality. The loss or unavailability of this information could have a significant impact upon business operations. For this reason, Propio uses well-known cloud services for maintaining high availability (fault tolerant).

9.1 Policy

Propio has a *Information System Contingency Plan* ("The plan") for ensuring the continuity of business operations in the event of an emergency. Reference the plan for additional details including the documented recovery strategies. The plan includes:

- Identification of the criticality of information resources
- Documentation of how data is backed up (maintaining availability through redundancy)
- Periodic testing or conducting tabletop exercises and revision of plans

Note: *This could be in the form of documenting any planned downtimes as a partial test of the disaster recovery plan.*

9.2 Procedure

9.2.1 Criticality Analysis and/or Business Impact Analysis

An inventory of information resources that contain confidential information is maintained in the *Business Continuity and Disaster Recovery Plan.* The criticality of these systems is based on the maximum time they could be down without serious impacts on business operations.

9.2.2 Unplanned Downtimes

Whenever a Propio system goes down, the workforce will be expected to implement their contingency plans, also known as "downtime procedures."

9.2.3 Data Backup Plans

The type and frequency of backups is documented in the *Business Continuity and Disaster Recovery Plan.* In case of failure, the Propio environment can be rebuilt from backups.

9.2.4 Disaster Recovery Plans

Reference the *Business Continuity and Disaster Recovery Plan*. The original plan along with any revisions are retained for six years from the date of its creation or update.

9.2.6 Testing and Revision

Testing is used to identify gaps in the plans and make any necessary revisions to the process. The disaster recovery is tested annually through tabletop exercises. Partial testing on plans may include documenting each time a system is successfully recovered after a planned or unplanned downtime.

9.2.7 Staff Training

The members of the Incident Response Team (IRT) receive periodic education and training on the disaster recovery plan.

10.0 Physical Security

Physical security ensures the appropriate protection of people, facilities/buildings (corporate-owned or leased buildings), information systems, and their supporting infrastructures against physical threats.

All of Propio's applications and systems are remotely cloud hosted inside the Amazon Web Services (AWS) Cloud.

10.1 Policy

Physical security safeguards and controls have been documented in the *Facility Security Plan*.

Members of the workforce are responsible for physically securing their work environment. However, the protected health information (PHI) of clients resides in a securely hosted environment. Therefore, PHI should not be printed or stored on a workforce member's computer.

10.2 Procedure

10.2.1 Access Controls to Restricted Access Areas (Office Areas and Data Centers)

Cloud vendors (Microsoft, Amazon, and Twilio) used by Propio for hosting applications and systems, have their own strict physical security controls that have passed several industry certifications for security and compliance.

Propio is responsible for some physical security measures at HQ. Secure areas (IDF) have limited access ((4) FTEs + CTO and CEO); (2) have door keys.

Territorial Restrictions: No data (in direct control of Propio) is stored outside of the continental United States. Cloud vendors are contractually obligated to honor Propio's US boundary restrictions. There is no offshoring of PHI. Some HR/PII data may be housed in SharePoint (O365)

10.2.2 Responsibilities for Physical Security

Aside the cloud-based hosting vendors, each workforce member has the responsibility for physically securing their work environment. For workstations and Laptops, write to optical and write to USB is capability is disabled. Access to personal webmail and social media are blocked. Bit locker full disk encryption is applied with passwords sync'd to the AD account; O 365 uses MDM to achieve a remote wipe (upon reported loss or theft).

10.2.3 Maintenance Records

The HIPAA Security Rule's addressable implementation specification: *Maintenance records §164.310(a)(1)(iv)* requires repairs and modifications related to restricted access areas need to be maintained. Because Propio uses cloud vendors for hosting its applications and systems, compliance with this requirement is the responsibility of Propio's vendors (Amazon, Twilio, and Microsoft) and attested to in their annual SOC 2 Type 2 reports.

11.0 Device and Media Controls

Inadequate security of workstations, mobile devices, and media could expose Propio to such risks as malicious code, unauthorized access, loss of data, and theft. Therefore, devices and media containing confidential information must be protected from unauthorized access, use, or disclosure.

In this manual, the term *devices* includes:

- Workstations or laptops
- Tablets or smartphones
- Printer (MFP) Scanners/printers (which are locked down to only Propio email domain)

In this manual, the term *media* includes:

- USB memory devices such as thumb drives, flash disks, jump drives, etc.
- CDs and DVDs
- Computer hard disk drives
- Portable, external hard drives

11.1 Policy

Propio's *Workforce Policies on Privacy and Security* specifically states that protected health information (PHI) or personally identifiable information (PII) is to be stored in Propio's applications or secure file storage system in the cloud and not on any user-owned device or portable media. However, if the need ever arises to do so, encryption must be used to protect the data at rest.

Additionally, Propio requires an encrypted hard drive is required for workforce-owned devices used to access Propio software or a client's system. This was done for two reasons:

1. Meets client security expectations
2. Reduces the risk of ransomware controlling access to stored data
3. Note: Some workers may be required to use AWS workspace (designed for contactors). Employed workers are provisioned with a company-issued device

Any media that could possibly contain confidential information must be sanitized or erased before the media is reused or disposed.

Tools/processes to be used: ConnectWise Automate 3rd Wall are used to enforce USB restrictions and/or block. Bitraser data eraser is used to certify the destruction of data; Propio uses on USB media as required.

11.2 Procedure

11.2.1 Security Controls (Required and Recommended)

A list of the general security control standards for workstations, laptops, tablets, and smartphones are provided at the end of this chapter. The Chief Information Officer (CTO) determines the level of residual risk that the organization is willing to accept to maintain a balance between user functionality and security.

11.2.2 Workstations and Laptops

Only contractors may use personally-owned workstations or laptops used for conducting Propio business and via the AWS Workspace (virtual desktop). Expectations for contractor's work environment security are defined in the *Handbook, workforce policies are* reinforced through policy and annual awareness training (new hire training.) Security controls are outlined in Figure 11.1 *Security Configurations* at the end of this chapter.

All employees use Propio-issued assets (workstation and/or laptop) if they are part of the mobile workforce. Propio requires all employees issued a laptop to take their laptop home at night.

11.2.3 Mobile Devices

Propio supports a Bring Your Own Device (BYOD) plan for smartphones. Mobile Device Management (MDM) software is used to enforce security settings. The controls listed in Figure 11.1 *Security Configurations* at the end of this chapter are general recommendations for any smartphone or tablet user.

11.2.4 Encryption (Data at Rest)

Media containing confidential information needs to be encrypted to protect data from unauthorized access. Wherever possible, encryption methodologies should be validated as compliant with Federal Information Processing Standards (FIPS) Publication (Pub) 140-2.

Without encryption, Propio could be subject to costly and time-consuming breach notification requirements if a breach were to occur. Reference: *Breach Notification for Unsecured Protected Health Information (45 CFR Parts 160 and 164), amended by the Omnibus Rule.*

11.2.5 Retention

Media containing official records will be retained in accordance with federal and state regulations and Propio's contractual obligations. Data are retained on a case-by-case basis, per contract. Generally, contracts require the destruction of customer data within 30-90 days after contract expiry.

11.2.6 Reuse and Sanitization

If media will be reused, stored data belonging to Propio must be removed and the media sanitized. Sanitization is the process of removing information from storage media. This may be accomplished by:

1. Using "delete" or "erase" commands to remove files
2. Reformatting the media
3. Overwriting the media several times with random patterns of 1s and 0s (use utility programs such as KillDisk to wipe (sanitize) hard disk drives; use only tools that are compatible with DoD 5220.22-M specification for sanitization.
    a. Where possible, use tools and processes that provide a certificate of erasure while documenting the number of passes, the method and type selected for the wipe

b. If the process is outsourced to an e-destruction vendor, ensure they destroy media onsite (ideally) and provide a certificate of destruction (e.g., Iron Mountain)

11.2.7 Disposal

The memory must be erased (hard reset) before reuse or disposal of devices or media.

11.2.8 Legal or Litigation Hold (eDiscovery)

Propio will preserve records when there is reasonable anticipation of an investigation, audit or litigation involving the records or when an official litigation hold has been received. Relevant records will be placed under a legal hold and normal destruction practices will be suspended. The CTO will closely follow the guidance provided by legal counsel to implement the appropriate safeguards and controls to preserve the information from loss, destruction, or alteration. Normal retention and destruction processes may resume once the receipt of a written notice from legal counsel has been received stating that the legal hold has been lifted. Propio is expected to leverage E5 O365 tools to complete eDiscovery and litigation holds while adhering to prevailing practices. Veeam backups for O365 will be utilized to store the results

11.2.9 Software

Workforce members must stay current with appropriate software patches and security updates to their devices. Software use must adhere to the software license agreement. ConnectWise Automate is used to enforce patch frequency and latency requirements. Patches are deployed on a priority basis; critical patches are to be deployed as close to immediately as is possible (generally after testing for 2 weeks); drivers are manually released, as needed.

11.2.10 Accountability

If needed, the Information Security Officer will determine the process for maintaining accountability per HIPAA's Security Rule §164.310(d)(2)(iii) *Accountability*, if, in the rare event, the equipment or media stores PHI or PII.

Figure 11.1 – Security Configurations

Technical controls	Cloud Workstation	User Laptop / Workstation*	Smartphone/ Tablet **
Password protection or biometric, or a screen unlock pattern feature access for booting or powering up the device	Yes	Yes	Yes
Memory is automatically erased after ten unsuccessful logon attempts			Yes
Antivirus and/or endpoint security software	Yes	Yes	No
Maintain updated antivirus software	Yes	Yes	
Maintain the latest version of operating system, patches, and security updates (only OS version that support the MDM tool will be supported)	Yes	Yes	Yes
Endpoint protection for detecting adware, spyware, and other malicious code	Yes	Yes	No
Personal firewall software	Yes	Yes	
Encryption for stored data (data at rest)1	Yes	Yes	Yes
Configured to prevent auto run of executable programs from the USB port	Yes	Yes	
Activate password-protected screen savers after predefined period of inactivity (e.g. 10 minutes) to prevent unauthorized access	Yes	Yes	Yes
Remove unneeded services or programs from device – rooted (jailbroken) devices are not permitted to enroll and are not allowed to function after enrollment	Recommended	Recommended	Yes

Notes: * The laptops/workstation used by the employed workforce are primarily Propio-issued. For the personal assets that are permitted (contractors), they are provisioned with a secure virtual desktop via AWS Workspace.

** Personally-owned smartphones are permitted to be used for conducting Propio business. The controls listed on this page are enforced.

1 Workforce members are strongly discouraged from storing any confidential information on the internal hard disk drive of their workstation, laptop, or in the memory of a tablet or smartphone.

In the rare event that any mobile device stores Propio's confidential information, the two following requirements must be met:

1. Power-on password, passcode, or some other type of authentication of the owner
   Note: *For most devices, enabling this feature will automatically encrypt the device's internal memory or a memory card.*
2. Automatic time out or locking of the device after 15 minutes of inactivity (or sooner)

12.0 Network Security

Propio uses Microsoft O365 for hosting for its network domain. Propio has contracted AWS to host their data center and the Propio software stack. Microsoft and AWS have several certifications that can be found on their websites. These cloud vendors offer network monitoring and protection from hacking and Distributed Denial of Service (DDoS) attacks. Both cloud service providers have a Shared Responsibility Model for protecting the network domain. Shared responsibilities include patch management and configuration management.

12.1 Policy

The Chief Information Officer (CTO) is responsible for Propio's network domain and connectivity to the Propio software.

By default, access controls for network domain will be set to "deny all," unless specifically allowed Secure Internet protocols are used for transferring data securely in and out of the network.

12.2 Procedure

12.2.1 General Network Security Practices

Network security at Propio follows generally accepted practices that include, but are not limited to:

- Maintaining high availability by eliminating single points of failure where feasible
- Using strong passwords for administrator accounts
    - Centralized authentication is used for both general user access and privileged administrative accounts. Propio separates privileged administrative accounts from general user accounts; i.e., provisioning an IT administrator at least two accounts: one account for use completing day-to-day activities and a separate administrative account with access only to systems required by the IT administration function
- Auditing and monitoring operating system and application server logs as well as network traffic and reviewing event logs as needed

  Note: *Propio leverages O365 logs and platform-centric logs today. SIEM tools is planned. Current and future tools and processes are configured to automatically notify network engineers and other assigned/authorized technicians when suspicious activity is detected, or an alarm is activated.*
- Running services only as required for functionality or administration
- Restricting IP addresses
- Maintaining current network drawings (ideally automated but at a minimum, manually generated)
- Filtering Internet activity to prevent access to unauthorized or inappropriate websites (Palo Alto URL filters)
- Scanning inbound and outbound traffic (packets, protocols, data file transfers, etc.)

12.2.2 Network Segmentation

The internal network is divided into sub-networks for performance reasons and for security. Segmentation can limit the scope of an information security incident. Network

segmentation means that each subnet exists within a “boundary of trust.” Checks should be made for any incoming and outbound traffic (packets, protocols, data file transfers, or user access) that crosses the boundary.

Virtual Local Area Networks (VLANs) or separate networks will be used to segment certain types of equipment and devices including biomedical equipment and equipment used to process credit card transactions.

Propio highly segments higher-risk environments to provide trust zones for developers, employees, servers, prod-to-prod traffic. VPN access is assigned per role. Segmentation for VoIP (using MS Teams), conf. rooms, guest networks (so employees can use personal cell phones) are also implemented and maintained.

12.2.3 Transmission Security

Propio practices for transmission security:

- Installing an approved firewall between trusted and untrusted networks
- Placing devices connected to the Internet inside the DMZ (Demilitarized Zone) to provide better protection of the server and the network and to isolate connections to vendors and other partners
- Encrypting data transmissions or files containing confidential information including protected health information (PHI) and credit card data and using such security protocols as SSL/TLS, HTTPS, or IPsec to prevent unauthorized access and to preserve data integrity during transmission over open, public networks
- Email encryption uses the Office 365 Message Encryption (OME) option which is built into the system and enabled by the Azure Information Protection license for all the users. A “[key word]” in the subject line is used to enable encryption with receiver authentication required. TLS handshake is enabled for opportunistic encryption
- Note:Propio would be subject to costly and time-consuming breach notification requirements if a breach were to occur without appropriate encryption technologies in place. Propio encryption standards are selected to meet Federal Information Processing Standards (FIPS) 140-2.
- Site-to-Site VPNs are in use (using IPsec encryption) at HQ and Data Centers

12.2.4 Wireless (Wi-Fi) Network Security Controls

Propio manages (4) wireless networks, including one guest network . The workforce is responsible for securing the wireless networks that they use within their home or office in a manner that protects confidential information from unauthorized access or eavesdropping. Wireless connections must employ industry-standard encryption (WPA2 and HTTPS). Propio is currently using a pre-shared key and plans to migrate to Radius and LDAPS, soon.

13.0 Security Architecture

Secure system design and management reduces risks. For that reason, the security architecture of information systems is fundamental for ensuring security.

13.1 Policy

Propio uses Microsoft Azure and Amazon Web Services (AWS) cloud hosting services for hosting for its network domain, the Propio software, and other electronic files needed for running the business. Therefore, most of the security architecture is the responsibility of those vendors. The level of protection provided is commensurate with the identified risks.

13.2 Procedure

13.2.1 Separation of Duties (aka segmentation of duties)

Separation of duties requires dividing the various roles and responsibilities and implementing a structure of checks and balances so that a single individual cannot subvert security. The CTO ensures reasonable measures are taken to ensure separation of duties. Because of the limited size of IT support staff at Propio, full separation of duties may be challenged. Currently, reasonable segmentation is in place for the Server, Network, Desktop, Developers, Leadership, and Help Desk Staff.

13.2.2 Server Setup

Propio owns the hardware within its Mastin and Guadalajara offices. These locations host the corporate network. All production environment equipment is hosted in AWS and Twilio cloud locations. Document storage is located inside the Microsoft 365 environment using SharePoint.

13.2.3 Antivirus Software and Patch Management

Servers in the Mastin and Guadalajara offices are managed by Propio using Microsoft Defender (antivirus) and ConnectWise Automate (patch management) tools. Systems are regularly patched and monitored for on-premise, data center-hosted, and SaaS vendors (under contract) against known vulnerabilities.

3rd party application vulnerabilities are also patched regularly via ConnectWise Automate

13.2.4 Configuration and Change Management

Propio manages code releases and infrastructure changes formally via a Change Advisory Board and supporting process

Modification of the Propio software and the production environment follow the established change control process specified in Chapter 14, *Change Control and in the Software Development Life Cycle (SDLC) Policy*. The change control process includes determining if the configuration management database needs updating.

13.2.5 Application/System Access Controls

Applications and information systems use technical controls for restricting access, and by default, denying access unless properly authenticated. Applications and systems used by Propio:

- Support assignment of unique user profiles or identifiers (user IDs) that hold persons and entities using the system accountable for their actions (Please see Chapter 5, *Access Control* for additional information)
- Enable system logging or auditing to hold the workforce accountable for the data and information they access (Please see Chapter 7, *Security Monitoring and Auditing* for additional information). Propio manually monitors failed authentication attempts and AD group membership changes. Automated tools are being considered in the future.

13.2.6 Environments

Test, development, and/or training environments are logically separated from the production environment. The test, development, and/or training environments do not have access to production database unless they are strictly controlled. These segments are "zoned" w/VLANS to prohibit cross communication.

Any environment using identifiable (and sensitive information) must be approved by the CTO and must enforce the same security safeguards and controls that apply to the production environment. Propio maintains a limited and approved access control list (employees only – no contractors) to sensitive environments. In addition, role-based VPNs are used to control access to the minimum necessary and need to know.

13.2.7 Identification, Authentication, and Authorization

Application or system authentication as well as the password standards described in Chapter 5, *Access Controls*, will be followed. Passwords are encrypted during transmission and rendered unreadable when stored within applications or systems.

A limited number of people have administrator access at the "root" level. To prevent the potential compromise of multiple systems, the same administrator password will not be reused across multiple applications or systems. Default accounts are removed, disabled, or at the very minimum, have the default passwords changed. Propio uses a password vault to ensure access to privileged credentials with a "break the glass" process to ensure Sr. leadership has access, if needed

User accounts automatically locked after five failed login attempts. RSA MFA- is the same

Access rights of the workforce and vendors are authorized to access only the systems and resources required for them to perform their duties with the minimum necessary level of privileges. Please see Chapter 5, *Access Control* for additional information.

13.2.8 Automatic Logoff

Automatic logoff means automatically terminating a user session after a predetermined period of inactivity. The automatic logoff feature ensures that confidential information will be protected in the event the user fails to log off. Automatic logoff time intervals are set based upon risks.

Propio standards include:

- **VPN** is 1-hour
- **Endpoints:** Endpoints are set to timeout after 15 minutes of inactivity (servers, desktops, laptops). While the workforce are required to log off an information resource or lock the workstation (via windows password-protected screensaver) whenever they leave their workstations unattended for an extended period of time, automatic logoff serves as an additional layer of security.

For information resources that lack automatic logoff, some other type of compensating control could be implemented to meet the intent of automatic logoff. Please see Chapter 5, section 5.2.6, *Automatic Lockout (End user devices)*.

13.2.9 Auditing and Monitoring

An audit trail will include sufficient information to establish what events occurred (type of event, when the event occurred, etc.). The Chief Information Officer (CTO) will ensure that audit logs are maintained and protected from unauthorized access or destruction. For more information, please refer to Chapter 7, *Security Monitoring and Auditing*.

The Privacy Officer along with the CTO will determine which user activities to audit.

13.2.10 Data Backup Plans

The CTO will determine the appropriate data backup plans. Please see Propio's *Business Continuity and Disaster Recovery Plan* for additional details on data backup plans. The backup plan is generally described as follows:

- Nightly backup jobs are performed by Propio staff (stored in the contracted cloud service)
- SQL server for the Propio ONE application is backed up with both daily full backups and incremental backups that are conducted more than once per day.

Propio does not use any type of portable or removeable media for its data backups; therefore, a chain of custody for backup media and final disposition is not necessary, beyond what is specified within the service contract with cloud vendors. All laptops desktops and servers are set to read but not write (removable media)

13.2.11 Accountability for the Movement of Information Resources

Because Propio relies on cloud service providers with a high-availability support model, the HIPAA Security Rule criteria for performing data backups of systems that store or process protected health information (PHI) before being moved is not applicable. For systems that Propio is directly responsible for, Propio will provide a compliant backup, before moving the hardware.

13.2.12 Integrity

Inaccurate information can affect business decisions. If the data values stored in a database are incorrect or have been altered, then the database is said to have lost its data integrity.

Most software applications and communications protocols automatically check for certain errors that could cause integrity problems. The following are recommended security controls to maintain the integrity of information:

- Testing applications and systems for accuracy as well as functionality before they "go live"
- Using encryption to preserve the integrity of data as it passes between systems
- Checking for possible duplication of data, especially between two systems
- Employing antivirus software to detect and prevent malicious code from altering data
- Checking for data synchronization errors
- Maintaining logs of sysadmins and data base administrators (DBAs) activities, traced to individuals

Flaw Remediation:

- Identifying, reporting, and correcting Information system flaws (i.e. , completing vulnerability scans and addressing flaws)
- Testing software and firmware updates for effectiveness and potential side effects before installation
- Incorporating flaw remediation into the organizational configuration management process

Malicious Code Protection:

- Deploying NextGen Anti-virus tools with current updated virus definition (DAT) files.
- Ensuring DAT files are updated regularly
- Periodically scanning Information systems and components for malicious code
- Ensuring administrators are notified - and they respond to malicious code detections

Information System Monitoring:

- Monitoring information systems to detect attacks, potential attacks, and unauthorized use (This can be done through audit activity in real time, monitoring devices, or applications such as Tripwire or SiteScope.)

Security Alerts, Advisories, and Directives:

- Receiving and/or subscribing to external security alerts, listservs, etc. related to the information system? For instance, do vendors notify you of security issues with an application?
- Generating and disseminating internal security alerts, advisories, and directives as deemed necessary

Software, Firmware, and Information Integrity:

- Using integrity verification tools to detect unauthorized changes to software, firmware, and information (e.g., Tripwire)

Phishing and Spam Protection:

- Employing spam/phishing protection mechanisms and keeping them updated as needed

Information Handling and Retention:

- Handling information within and from outputs - and retaining data for the amount of time as required by data policies, regulations, and contracts

Additional Integrity controls for data at rest include:

- TCP/IP Cyclical Redundancy Checks (CRCs)
- SAN/RAID storage, read after write verification
- Use of solid-state drives
- Error Correcting Code (ECC) memory in servers
- Application layer and database controls
- Backups
- Periodic audits

13.2.13 Certificate Management

If digital certificates are used for production systems, the certificate should have an expiration date. It is the CTO's responsibility to renew certificates before they expire. Propio uses self-signed (internal) and commercial (public facing) SSL certificates; GoDaddy and Lets Encrypt are used. Propio uses Outlook calendar for tracking certificate expiry.

13.2.14 Encryption Key Management

Encryption keys are managed by the CTO and are stored in a secure location. Propio uses Keeper Enterprise Password Vault.

13.2.15 Termination of System Administrators

The following actions are taken before someone with system administrator privileges terminates their employment with Propio:

- Access to the Propio software and its clients' information resources must be terminated
- Any confidential information, including proprietary data or software code that may have been in their personal possession, must be returned or destroyed
- Passwords or encryption keys must be made available to the Chief Executive Officer (CEO) of Propio
- Password vault information is transferred to Director of Global IT.
- Return of assets

14.0 Change Control

The structured change control process followed by Propio ensures that changes are requested, reviewed, tested, scheduled, communicated, implemented, and documented in a consistent manner.

14.1 Policy

The change control process outlined in this chapter will be followed to ensure that changes:

- Are reviewed, evaluated for possible risk and impact, tested, and approved in advance
- Are communicated to clients and the workforce when needed
- Happen in an orderly fashion and during a time to minimize the impact to users
- Do not unintentionally diminish the confidentiality, integrity, and availability of systems
- Ensure backups are completed before critical changes are executed

14.2 Procedure

14.2.1 Change Control Process

Changes to Propio information resources are managed in accordance with the following procedures:

- Change requests are submitted using Azure DevOps or a *Change Control Request* form
- Change requests will be reviewed by the Change Advisory Board (CAB)
- If the change request is not an "Emergency," (reference the table below) the change request will be reviewed with the Chief Information Officer (CTO) and other Propio staff as needed
    - The greater the risk and impact, the greater the scrutiny for the change request
- If approved by the CAB (one Developer and 1 Infrastructure SME) or CTO, the change will be tested before being promoted to Production
- ***Note:*** *Changes to the test environment are also tightly controls (the worker executing the change must be an employed worker form the development network (access control is enforced at the router)*
- Schedule and implement changes with little or no impact to users; otherwise, communicate the change to the appropriate users
- If any problems are encountered with the change, the change will be backed out and investigated for the root cause of the failure
- A history of changes to the Propio software is tracked using Azure DevOps repository is used for version control and source code management

Patches/updates that occur automatically (e.g., Microsoft's Patch Tuesday and antivirus definitions and updates – Reference section 13.2.3 of this manual) do not need to go through change control.

Type of Change	Description
Routine	Common, incremental updates, small new features, data fixes, etc., with little or no downtime, minimum resources required and a high level of confidence that the change will be successful. Most changes fit this category.
Moderate	Resources are required, some downtime involved, and changes will not significantly change the functionality of an application or system. This change introduces a moderate amount of risk to the organization.
Significant (or Critical)	Severely affecting some key users or affecting a large number of users. The risk and impact are high to medium, requires adequate resources and planning.
Emergency	Unanticipated changes that must be implemented immediately because the potential impacts for not implementing outweigh the risks associated with bypassing the formal change control process.

14.2.1 Emergency Change Control Process (emergency = eCAB)

Changes that are categorized as “Emergency” are changes that are made immediately to respond to a threat or major business interruption. Because this bypasses the normal change control review process, “Emergency” changes should be rare exceptions. The standard approval authority includes vote from (1) assigned SME from Development + (1) assigned SME from Infrastructure or approval from the CTO) – in accordance with figure 14.1 below:

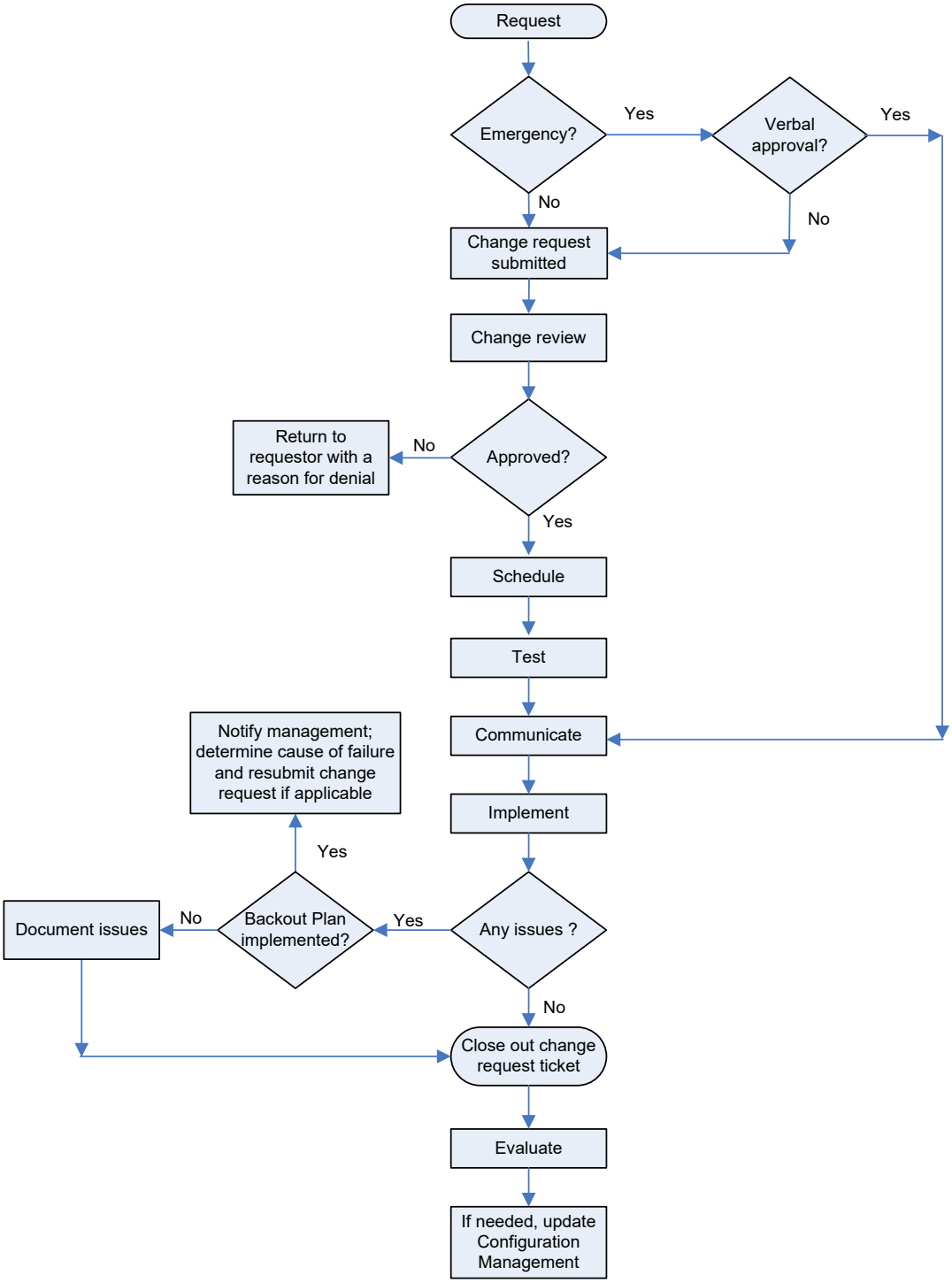


Figure 14.1 – Change Control Workflow Process

15.0 Configuration Management

Because the computing environment is constantly changing it creates challenges in maintaining accurate information about system configuration. Configuration management is the process of collecting and documenting specific information regarding each information resource toward gaining better control and oversight. This information has proven to be valuable, especially for:

- Supporting the goal of maintaining “high availability”
- Tracking accurate information on current system configurations (which can be useful for patch management, incident response, and disaster recovery)
- Making informed business decisions regarding upgrades or applying security patches
- Maintaining consistency in the configuration of servers, workstations, operating systems, and other components of the computing environment against known vulnerabilities
- Planning expenditures by centrally tracking warranty information and normal life-cycle replacements

A comprehensive and accurate configuration management system can help determine whether all existing systems are accounted for when researching and processing information on patches and updates.

15.1 Policy

Propio will maintain control over its information resources by tracking those resources in a configuration management database, spreadsheet or some other type of configuration management tool. Figure 15.1 outlines some of the information generally collected within a configuration management database.

The IT Department is responsible for developing processes for the implementation of patches and updates to systems. Security patches and system and software configuration changes will be evaluated and tested before deployment. System administrators will verify that applying a security patch will not void any warranties with vendors before applying a patch.

The process described in Chapter 14; *Change Control* must be followed before applying software patches to production systems. Changes to the production environment may require updates to the configuration management database.

15.2 Procedure

15.2.1 Configuration Management

The IT Department will create and maintain a configuration management process to ensure:

- A complete accounting of IS information resources (assets) are recorded in ConnectWise Automate, Auvik and MDM (or other) tools for:
    - Endpoints
    - Mobile Devices
    - Servers
    - Infrastructure

- Accuracy of information related to system configurations (which can be useful for patch management, incident response, and disaster recovery)
- Efficiency in expenditure planning by centrally tracking warranty information and life-cycle planning

Figure 15.1 outlines some of the information generally collected for configuration management.

15.2.2 Patch Management

Various sources exist for both security vulnerabilities and the associated fixes or patches, including:

- Vendor supplied patches or updates
- Vulnerability scanning tools (Nessus-like tools)
- Public websites and mailing lists including SANS (@Risk) or Bugtraq

The IT Department is responsible for:

- Keeping up to date on newly released patches and security issues
- Evaluating patches to determine relevancy to systems and applications used by Propio
- Determining significance and priority for applying a patch based upon:
    - Verification of the patch's source and reported criticality (e.g. high, medium, low) from reliable sources or vendors
    - Results of running a vulnerability scanner (Vulnerabilities identified as “high” risks should be addressed as soon as possible while the vulnerabilities identified as “low” can either wait or be ignored)
    - System criticality and system exposure (e.g. external facing systems versus internal file servers versus computer workstations)
- Determining which systems need to be patched for a given vulnerability or bug
- Testing updates using as many variations of production-like systems as possible to ensure smooth and predictable rollouts
- Submitting a change request (when needed)
- Limiting the number of individuals permitted to apply patches
- Scheduling based upon:
    - The urgency for installing the patch (infrastructure servers are typically patched when a reboot can be performed)
    - A phased approach (will the patch be pushed to all workstations at the same time or completed in phases to avoid overloading the network)
- Verifying the success of the patch related to:
    - Errors (For example, no reported issues within a week of patch application.)
    - Compliance (For example, are the systems actually patched? Is there a justification for any of the systems that were knowingly excluded from

receiving the patch that has been documented in the configuration management database?)

- Closing the patch management process by updating the configuration management database
- Building new, or updating, images and scripts to ensure that all newly built systems (servers, computer workstations, etc.) are appropriately patched

Sample: Configuration Management – Database Information

Equipment Identification

Name (device name as assigned by Children's)
Type of device (server, switch, firewall, SAN, etc.)
Location (building, rack, position within the rack)
IP address(es) and MAC address
Application(s) supported
Departments affected by outage
Restoration priority

Configuration

Hardware

Make/model
Vendor

Operating System

Name and version
Service pack and/or patch level
License key code

Software

Application(s) name(s) and version and current revision level
Application(s) vendor(s)

Procedures

Shutdown procedures
Startup procedures
Backup procedures
File restoration procedures
Problem resolution and escalation procedures

Contact Information

Primary and Secondary System Administrator(s) (name, phone numbers, email)

Figure 15.1 Sample Information for a Configuration Management Database

16.0 Security Evaluation

Managing risks appropriately requires knowledge of how security controls are deployed so that informed decisions can reduce organizational risks to an acceptable level. An *evaluation* is a review of technical and non-technical controls of an information security program. Evaluations are conducted periodically to:

- Assess the effectiveness of existing safeguards and controls
- Verify compliance with security policies
- Confirm regulatory compliance
- Identify weaknesses that represent potential vulnerabilities
- Document exceptions

Conducted by a technical specialist or a certified information security professional, *technical evaluations* may include vulnerability scanning and periodic penetration testing. Technical evaluations are useful for:

- Verifying the effectiveness of controls
- Detecting vulnerabilities in applications and systems; identify potential security risks that may be exploited
- Preventing security incidents and privacy breaches

A *non-technical evaluation* may include:

- Self-assessment or gap analysis against regulatory requirements
- A review of policies, procedures, and plans to validate that they have been periodically reviewed, updated, and approved
- Verification of security control settings
- Confirmation that the workforce understands and follows security policies
- A review of contracts or arrangements to ensure security requirements are met
- Review of users with elevated or privileged access

16.1 Policy

To ensure compliance with Propio security policies and regulatory requirements, the technical and non-technical security controls used by Propio will be evaluated annually.

16.2 Procedure

16.2.1 Evaluation – Non Technical

Figure 16.1 illustrates the evaluation and security management process.

Beyond compliance, evaluations may be based on generally accepted security practices from:

- The *HIPAA Audit Program Protocol* used by HHS Office for Civil Rights (OCR)
- National Institute of Standards and Technology (NIST) and documents created by the Department of Health and Human Services (HHS) and/or the Centers for Medicare and Medicaid (CMS)
- Center for Internet Security (CIS) Top 20 Critical Security Controls
- Health Information Trust Alliance Common Security Framework (HITRUST CSF)
- Health Industry Cybersecurity Practices (HICP), Section 405(d) “Aligning Health Care Industry Security Approaches” of the Cybersecurity Act of 2015 (Public Law 114-113)

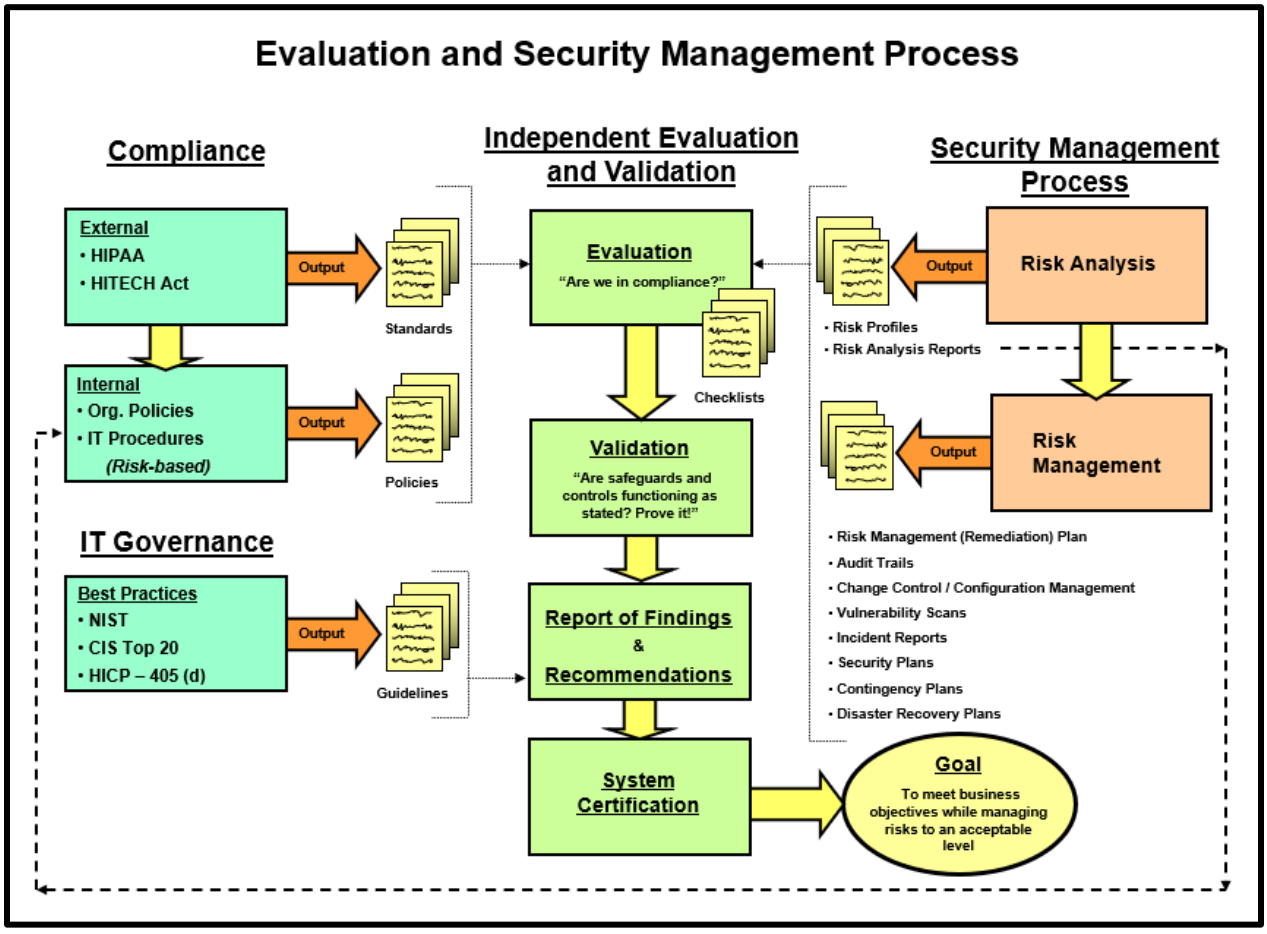


Figure 16.1 – The Evaluation and Security Management Process

16.2.2 Evaluation – Technical

Per chapter 4 section 4.2.7, *Vulnerability Scanning and Penetration Testing*, the Azure Defender for virtual machines environment is configured through the Security Center for an integrated vulnerability assessment solution (Qualys). Azure Defender performs a scans every 4 hours.
Note: *This interval is a default setting and is not changeable by Propio.*

The Chief Information Officer (CTO) receives scanning reports and or notifications when a possible vulnerability has been identified. The CTO will determine if the vulnerability is:

- Applicable and
- When the vulnerability will be addressed.

Microsoft's Defender and/or ConnectWise Automate emails a ticket and flags the asset for remediation. If the asset is a workstation, the Help Desk team resolves. If the asset is a server, the ticket is escalated to the systems administration team (onsite or on call rotation staff.)

17.0 Exceptions for Noncompliance

Occasionally there are extenuating circumstances in which compliance with an established information security policy, procedure, or standard is not possible, feasible, or would adversely affect business operations. These situations may warrant an exception.

17.1 Policy

Requests for exceptions to security policies or standards are documented. The Privacy and Security Committee will assess the risks associated with the requested exception and make the determination if the request for an exception is approved or denied. Requests are to be documented in the XenDesk ticketing system; escalations are routed to the CTO for approval

Because exceptions place Propio at risk, approved exceptions should have an expiration date, forcing the request to be periodically reviewed to determine if an exception still is needed.

17.2 Procedure

17.2.1 Requesting an Exception

A written request (via XenDesk Ticket) is required for an exception must be made in advance to the IT Department w/escalation to the Director of Global IT or the CTO (if necessary) Please see Appendix E, *Security Exception Request* form.

17.2.2 Reviewing the Request

The request will be reviewed for its feasibility, risk, and impact. The Chief Information Officer (CTO) and the Information Security Officer (ISO) will initially review and if needed, the Privacy and other leaders will be consulted as appropriate.

If the request is denied, then the reason for the denial is communicated (in writing or verbally) to the original requester. The IT Ops/CTO will work with the individual requesting the exception on how best to bring them into compliance.

An approved exception will be retained by the CTO. One copy will be sent to the requester. The requests will be retained in XenDesk.

17.2.3 Expiration of an Exception

Approved exceptions should include an expiration date. The CTO will work collaboratively with the individual requesting the exception to set a reasonable expiration date for the exception. In most situations, the expiration date should not exceed one year. An ongoing exception may require a more permanent solution or change in a standard or business practice.

17.2.4 Annual Review of Exceptions

Exceptions should be reviewed on a periodic basis.

18.0 System Life Cycle Planning

To be effective, security is planned and managed throughout the life cycle of an information system or application. Security is addressed from conception or purchase through design, development, deployment, operation, and retirement from service.

18.1 Policy

Propio considers information security throughout the life cycle of its applications and systems.

18.2 Procedure

The information security assurance process defines a formal review process that ensures security is addressed during each phase of the system life cycle.

18.2.1 Life Cycle Phase 1 – Definition of Requirements

In this phase, those involved define the information and operational needs that should be supported by a new system or application. This phase should address high-level security questions, including:

- What is the sensitivity of the data being processed?
- Will the system or application need to interface with other systems or applications?
- Will the system or application be directly accessed via the Internet?
- Is encryption needed?
- What security features and controls are required?

18.2.2 Life Cycle Phase 2 – Evaluation of Systems or Applications

In this phase, commercially available systems or applications that meet the basic needs identified in Phase 1 are evaluated in detail. In addition to considering functionality from the users' points of view, systems or applications also will be evaluated to see if they include appropriate security features and have the flexibility needed to support Propio information security policies and procedures. A checklist can be used to evaluate the security controls in the contract negotiation before making a commitment. This is especially important for applications or systems remotely hosted or hosted in the cloud. See the Vendor Security Policy and Procedures for more information.

18.2.3 Life Cycle Phase 3 – Purchase, Lease, or Develop

If a commercial off-the-self (COTS) application or system has been selected, the next step in the life cycle process is to negotiate a contract to either purchase or to lease the software.

If the application is to be developed in-house, periodic code reviews should check functionality and security while the application still is in development. See the SDLC Policy and Procedures for more information

18.2.4 Life Cycle Phase 4 – Installation/Implementation

The installation and implementation phases should include the following steps:

- Perform functionality and performance tests to ensure requirements are met
- Configure the security features to meet Propio requirements
- Document configurations
- Set up new user accounts, including unique user IDs and passwords
- Create departmental contingency plans for planned and unplanned downtimes
- Include the system in the disaster recovery plan
- Create user education and training plans
- Conduct a risk analysis and create a risk profile

18.2.5 Life Cycle Phase 5 – Operation and Maintenance

Security is just as important during the operational phase as it is during earlier phases. This phase should include:

- Maintaining established security controls
- Conducting training for new users
- Auditing and monitoring
- Configuration management
- Media controls and data backup
- Recovery (when the system experiences unexpected problems)
- Vulnerability testing
- Updating the risk analysis and disaster recovery procedures if there are significant changes to the system, application, or environment.

18.2.6 Life Cycle Phase 6 – Retirement

This is the final phase of the life cycle, in which the system or application is retired from use or reaches “sunset.” Security considerations in this phase include the following:

- Evaluate legal requirements for records retention, if applicable
- Archive, back up, discard, or destroy data
- Shut down the system or application
- Sanitize equipment and media to overwrite confidential or sensitive data
- Follow disposal and/or transfer procedures for obsolete equipment

18.2.7 Records Retention

Propio official records will be retained accordingly as needed for running the business, meeting regulatory requirements (evidence of compliance), and as evidence for investigations or litigation.

The IT Compliance Manager will provide guidance on data retention, storage, and accessibility based on business and regulatory requirements. The retention of an official record will be extended indefinitely as long as Propio has reason to believe the records are relevant to an unresolved dispute, investigation or litigation hold. Confidential information, including PHI and personally identifiable information (PII) obtained by Propio will be securely disposed of after its use. For detailed information see the *Records Retention and Destruction Policy*.

Any policies, procedures, plans, educational materials or any other records that can be used as proof of compliance with HIPAA must be retained for six years.

Appendix A – HIPAA Security Rule

ADMINISTRATIVE SAFEGUARDS	
§164.308(a)(1)(i)	**Security management process**
§164.308(a)(1)(ii)(A)	Risk analysis *(Required)*
§164.308(a)(1)(ii)(B)	Risk management *(Required)*
§164.308(a)(1)(ii)(C)	Sanction policy *(Required)*
§164.308(a)(1)(ii)(D)	Information system activity review *(Required)*
§164.308(a)(2)	**Assigned Security Responsibility**
§164.308(a)(3)(i)	**Workforce security**
§164.308(a)(3)(ii)(A)	Authorization and/or supervision *(Addressable)*
§164.308(a)(3)(ii)(B)	Workforce clearance procedure *(Addressable)*
§164.308(a)(3)(ii)(C)	Termination procedures *(Addressable)*
§164.308(a)(4)(i)	**Information access management**
§164.308(a)(4)(ii)(A)	Isolating health care clearinghouse functions *(Required)*
§164.308(a)(4)(ii)(B)	Access authorization *(Addressable)*
§164.308(a)(4)(ii)(C)	Access establishment and modification *(Addressable)*
§164.308(a)(5)(i)	**Security awareness and training**
§164.308(a)(5)(ii)(A)	Security reminders *(Addressable)*
§164.308(a)(5)(ii)(B)	Protection from malicious software *(Addressable)*
§164.308(a)(5)(ii)(C)	Log-in monitoring *(Addressable)*
§164.308(a)(5)(ii)(D)	Password management *(Addressable)*
§164.308(a)(6)(i)	**Security incident procedures**
§164.308(a)(6)(ii)	Response and Reporting *(Required)*
§164.308(a)(7)(i)	**Contingency plan**
§164.308(a)(7)(ii)(A)	Data backup plan *(Required)*
§164.308(a)(7)(ii)(B)	Disaster recovery plan *(Required)*
§164.308(a)(7)(ii)(C)	Emergency mode operation plan *(Required)*
§164.308(a)(7)(ii)(D)	Testing and revision procedures *(Addressable)*
§164.308(a)(7)(ii)(E)	Applications and data criticality analysis *(Addressable)*
§164.308(a)(8)	**Evaluation**
§164.308(a)(8)(b)(1)	**Business associate contracts and other arrangements**
PHYSICAL SAFEGUARDS	
§164.310(a)(1)	**Facility access controls**
§164.310(a)(1)(i)	Contingency Operations *(Addressable)*
§164.310(a)(1)(ii)	Facility security plan *(Addressable)*
§164.310(a)(1)(iii)	Access control and validation procedures *(Addressable)*
§164.310(a)(1)(iv)	Maintenance records *(Addressable)*
§164.310(b)	**Workstation use**
§164.310(c)	**Workstation security**
§164.310(d)(1)	**Device and media controls**
§164.310(d)(2)(i)	Disposal *(Required)*
§164.310(d)(2)(ii)	Media re-use *(Required)*
§164.310(d)(2)(iii)	Accountability *(Addressable)*
§164.310(d)(2)(iv)	Data backup and storage *(Addressable)*
TECHNICAL SAFEGUARDS	
§164.312(a)(1)	**Access Control**
§164.312(a)(2)(i)	Unique user identification *(Required)*
§164.312(a)(2)(ii)	Emergency access procedure *(Required)*
§164.312(a)(2)(iii)	Automatic logoff *(Addressable)*
§164.312(a)(2)(iv)	Encryption and decryption *(Addressable)*
§164.312(b)	**Audit controls**
§164.312(c)(1)	**Integrity**
§164.312(c)(2)	Mechanism to authenticate electronic protected health information *(Addressable)*
§164.312(d)	**Person or entity authentication**
§164.312(e)(1)	**Transmission Security**
§164.312(e)(2)(i)	Integrity controls *(Addressable)*
§164.312(e)(2)(ii)	Encryption *(Addressable)*

Appendix B – Cross Reference to HIPAA Security

	IT Security Manual Chapter Title	HIPAA Citation	HIPAA Standard or Implementation Specification
1	**Introduction**	None	
2	**Responsibilities**	**§164.308(a)(2)**	**Assigned Security Responsibility**
3	**Security Training, Education, and Awareness**	**§164.308(a)(5)(i)** §164.308(a)(5)(ii)(A) §164.308(a)(5)(ii)(B) §164.308(a)(5)(ii)(C) §164.308(a)(5)(ii)(D)	**Security awareness and training** Security reminders (Addressable) Protection from malicious software (Addressable) Log-in monitoring (Addressable) Password management (Addressable)
4	**Risk Analysis and Management**	**§164.308(a)(1)(i)** §164.308(a)(1)(ii)(A) §164.308(a)(1)(ii)(B)	**Security management process** Risk analysis (Required) Risk management (Required)
5	**Access Control**	**§164.308(a)(3)(i)** §164.308(a)(3)(ii)(A) §164.308(a)(3)(ii)(B) §164.308(a)(3)(ii)(C) **§164.308(a)(4)(i)** §164.308(a)(4)(ii)(B) §164.308(a)(4)(ii)(C) **§164.312(a)(1)** §164.312(a)(2)(i) §164.312(a)(2)(ii) §164.312(a)(2)(iii) §164.312(a)(2)(iv) **§164.312(d)**	**Workforce security** Authorization and/or supervision (Addressable) Workforce clearance procedure (Addressable) Termination procedures (Addressable) **Information access management** Access authorization (Addressable) Access establishment and modification (Addressable) **Access Control** Unique user identification (Required) Emergency access procedure Automatic logoff (Addressable) Encryption and decryption (Addressable) **Person or entity authentication**
6	**Remote Access**	**§164.308(b)(1)** **§164.312(e)(1)** §164.312(e)(2)(i) §164.312(e)(2)(ii)	**Business associate contracts and other arrangements** **Transmission Security** Integrity controls (Addressable) Encryption (Addressable)
7	**Security Monitoring and Auditing**	§164.308(a)(1)(ii)(D) **§164.312(b)**	Information system activity review *(Required)* **Audit controls**
8	**Security Incident Response Procedures**	**§164.308(a)(6)(i)** §164.308(a)(6)(ii)	**Security incident procedures** Response and Reporting (Required)
9	**Business Continuity and Disaster Recovery Planning**	**§164.308(a)(7)(i)** §164.308(a)(7)(ii)(A) §164.308(a)(7)(ii)(B) §164.308(a)(7)(ii)(C) §164.308(a)(7)(ii)(D)	**Contingency plan** Data backup plan (Required) Disaster recovery plan (Required) Emergency mode operation plan (Required) Testing and revision procedures (Addressable)

	IT Security Manual Chapter Title	HIPAA Citation	HIPAA Standard or Implementation Specification
		§164.308(a)(7)(ii)(E)	Applications and data criticality analysis (Addressable)
10	**Physical Security**	**§164.310(a)(1)** §164.310(a)(2)(i) §164.310(a)(2)(ii) §164.310(a)(2)(iii) §164.310(a)(2)(iv)	**Facility access controls** Contingency Operations (Addressable) Facility security plan (Addressable) Access control and validation procedures (Addressable) Maintenance records (Addressable)
11	**Device and Media Controls**	**§164.310(b)** **§164.310(c)** **§164.310(d)(1)** §164.310(d)(2)(i) §164.310(d)(2)(ii) **§164.312(a)(1)** §164.312(a)(2)(iv)	**Workstation use** **Workstation security** **Device and media controls** Disposal (Required) Media re-use (Required) **Access Control** Encryption and decryption (Addressable)
12	**Network Security**	**§164.312(e)(1)** §164.312(e)(2)(i) §164.312(e)(2)(ii)	**Transmission Security** Integrity controls (Addressable) Encryption (Addressable)
13	**Security Architecture**	**§164.308(a)(1)(i)** **§164.310(d)(1)** §164.310(d)(2)(iii) §164.310(d)(2)(iv) **§164.312(c)(1)** §164.312(c)(2)	**Security management process** **Device and media controls** Accountability (Addressable) Data backup and storage (Addressable) **Integrity** Mechanism to authenticate electronic protected health information (Addressable)
14	**Change Control**	None	
15	**Configuration Management**	None	
16	**Security Evaluation**	§164.308(a)(1)(ii)(D) **§164.308(a)(8)**	Information system activity review *(Required)* **Evaluation**
17	**Exceptions for Noncompliance**	None	
18	**System Life Cycle Planning**	None	

Appendix B – *Continued from Previous Page*

Appendix C – Information Security Officer Responsibilities

Listed below are the primary responsibilities for the Information Security Officer – listed by common frequency.

Daily/As needed

- Direct and oversee the information security program at Propio
- Accept, investigate, respond, and manage reported information security incidents
    - Initiate an investigation and lead the information security incident response to address the situation
    - Ensure the prevention, detection, containment and correction of security incidents and privacy breaches
    - Conduct post-incident analyses to determine if security policies need to be updated or revised or if technical controls and/or safeguards need to be adjusted
- Ensure security is planned and managed throughout the life cycle of an information system or application – from conception through design, development, deployment, operation, and eventual retirement from service
- Respond to requests from covered entities (Propio's clients) or business partners regarding information security

Quarterly

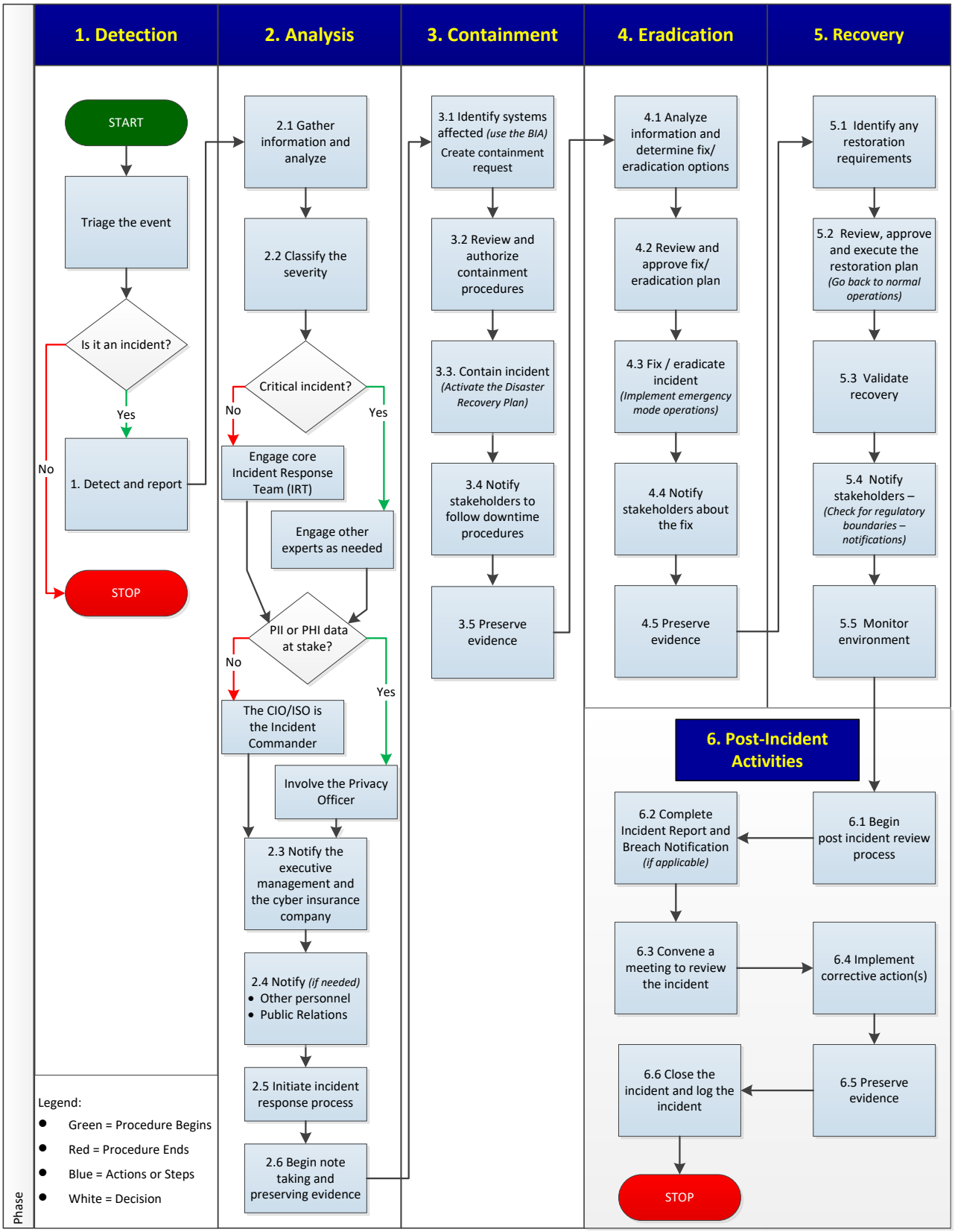
- Maintain workforce awareness in information security
    - Create and send out periodic security reminders to the workforce
- Review new or revised federal and state government healthcare laws and regulations pertaining to information security to determine if new policies or modifications of current policies are needed

Annually

- Develop, review, update, and implement compliance program and information security policies, standards, procedures, and plans
- Review and approve/disapprove requests for exceptions to the information security policies and standards
- Oversee the risk management program, which includes conducting risk analysis, implementing a plan to address identified threats and vulnerabilities that represent unacceptable risks and guiding the organization in enhancing security in a cost-effective manner
- Recommend appropriate security measures based upon risk and ensure the implementation of security safeguards and controls to reduce risks and/or to meet regulatory requirements
- Develop high-level plans for ensuring business operations in the event of an emergency
    - Support the development of a disaster recovery plan and a data backup plan
    - Conduct a tabletop exercise or test of the plans
- Evaluate regulatory compliance – either directly or through a third party
- Retain records and compliance documentation in accordance to records retention schedules

Note: *Proof of HIPAA compliance must be maintained for six years*

Appendix D – Incident Response (IR) Flowchart



Appendix E – Security Exception Request SAMPLE

Today's Date:	**Verbal Approval Date:** *(for emergency situations only)*	
Policy or standard:		
Situation Description: *(briefly describe the situation for which an exception or waiver is needed)*		
Negative Impacts: *(list the problems that will result if the policy is **not** waived)*		
Potential Risks: *(list the potential security risks if the policy is waived)*		
Affirmation:		
Requestor Name:		
Signature:	**Department:**	**Extension:**
Chief Information Officer (CTO):		❑ Approved ❑ Denied
Signature:	**Date:**	**Extension:**
Information Security Officer (ISO) :		❑ Approved ❑ Denied
Signature:	**Date:**	**Extension:**

Expiration Date: _____

Distribution: One copy to requester and one copy to Propio's secure document management/repository system.

Appendix F – Glossary of Terms and Definitions

Backup	A retrievable, exact copy of data.
Breach	The acquisition, access, use or disclosure of protected health information (PHI) or personally identifiable information (PII) in a manner not permitted (by law or regulation) which compromises the security or privacy of the PHI or PII.
Business Associate	An outside person or entity that performs a service on behalf of a covered entity that creates, receives, maintains, uses, discloses, or transmits protected health information (PHI).
Business Continuity	Ensures that critical business functions will continue to be performed during a business interruption and is normally a high-level plan.
Business Impact Analysis (BIA)	Facilitates business continuity and disaster recovery planning strategies by identifying an organization's critical applications and systems, estimating the potential impacts caused by a business interruption and determining the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
CFR	Code of Federal Regulations
Confidential Information	Any non-public information considered to be private or sensitive. Some examples of confidential information include: • Protected Health Information (PHI) – information about patients • Personally Identifiable Information (PII) – individual demographic identifiers including Social Security numbers (SSN) of workforce or patients • Financial information about the organization (checking account number, company credit card numbers, etc. • Passwords, PINs, or other security codes
Covered Entity	Healthcare providers, health plans or clearinghouses.
Disaster Recovery Plan (DRP)	A document that outlines a predetermined response to disastrous events and which describes the tasks and activities needed to recover to an acceptable level of operation
Disclosure	The release, transfer, provision of access to or divulging in any other manner of information outside the entity holding the information
Electronic Media	As defined by the HIPAA security regulations:

	(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper (via facsimile) and voice (via telephone) are not considered transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.
Electronic Protected Health Information (ePHI)	Individually identifiable health information that is transmitted by or maintained in electronic media as defined in federal law
Emergency Mode Operation Plan	A component of the business continuity plan that addresses access controls in emergency situations such as natural or man-made disasters whereby an organization would be able to continue to operate. (Source: Proposed HIPAA Security Rule) (See also Business Continuity Planning, Contingency Plan, and Disaster Response Planning)
Evaluation	A review of technical and non-technical controls of an information resource or an information security program aimed at assessing the fitness or efficacy of the controls. (See also Technical Evaluation and Non-Technical Evaluation)
Facility	The interior and exterior of a building or buildings and the surrounding grounds which are owned, leased, or controlled by Propio.
Facility Security Plan	A plan to safeguard the premises and building(s) (exterior and interior) from unauthorized physical access, and to safeguard the enclosed equipment from unauthorized physical access, tampering, and theft.
Health Information Technology for Economic and Clinical Health (HITECH) Act	Federal law enacted in February 2009 as part of the American Recovery and Reinvestment Act of 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules. (Source: HHS)

Health Insurance Portability and Accountability Act (HIPAA)	Federal law and regulations that require all covered entities and business associates to adhere to a minimum set of standards regarding the collection and processing of medical data and restricts the disclosure of such information. HIPAA created separate rules for Privacy, Security and Enforcement Rules, as well as the Breach Notification requirements under the Health Information Technology for Economic and Clinical Health Act (HITECH Act) regarding regulations for keeping patient information confidential and secure.
Incident	Any adverse event that threatens some aspect of information security, including loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. *(Not all incidents are breaches, however, all breaches start as incidents.)*
Information Resources	The collection of information technologies, (devices with computer chips that process and store information) and the information contained within these technology devices. More specifically, this means the information systems, infrastructure, applications, products, services, telecommunications networks, and related resources purchased by, leased, or operated on behalf of, or developed for the benefit of Propio.
Nonemployee	Includes anyone who is not part of Propio workforce: clients, contractors, vendors, etc.
OCR	Office for Civil Rights
Patch	A fix to a program. When used in the context of information security, the fix or patch mitigates a newly discovered vulnerability.
Penetration Testing *(Pen Testing)*	Process to evaluate a network's defenses by attempting to access the system from the outside using the same techniques that an external intruder (i.e., a hacker or cracker) would use.
Personally Identifiable Information (PII)	Any data that could potentially identify a specific individual. Examples of PII include, but are not limited to: • Name, such as full name, maiden name, mother's maiden name, or alias • Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number • Address information, such as street address or email address • Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry) • Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities,

	geographical indicators, employment information, medical information, education information, financial information). Source: NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
Power-On Password	Computer system will not boot without first entering a password.
Protected Health Information (PHI)	Under HIPAA, any patient information, whether oral or recorded in any form or medium, is required to be protected from all forms of unauthorized disclosure. In particular, any information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; the payment for the provision of healthcare services to an individual; and that identifies the individual or for which establishes a reasonable basis to believe the information can be used to identify the individual. (See also Electronic Protected Health Information, ePHI)
Recovery Point Objective (RPO)	The maximum loss of information related to backup frequency.
Recovery Time Objective (RTO)	The period of time within which systems, applications, or functions must be recovered to minimize the impact after an outage (A similar term that is commonly used is: *Maximum Allowable Downtime*).
Restricted Access Area	Areas of the facility where access is restricted to individuals with a legitimate "need to know."
Risk	The probability that a particular threat will exploit a particular vulnerability, or weakness, of a system.
Risk Analysis	The process of identifying threats, controls, and vulnerabilities and assessing the possible damage that could result if a threat successfully circumvents the existing controls and exploits the vulnerabilities.
Risk Assessment	Synonymous with Risk Analysis.
Risk Management	The process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk.
Role-Based Access	Access control based on specific rules relating to the nature of the person's job functions and the application/systems, which goes beyond simple worker identities.
Sanitization	Elimination of confidential or sensitive information from media.

Security Safeguards	Security policies, procedures, plans, standards and general measures used.
Service Account	An account that often is a built-in (domain and/or local) administrative level account that does not correspond to an actual person and is needed to perform certain automated activities or such executable programs as running batch files, backups, and system monitoring
Threat	A circumstance or event that has the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service.
Unsecured PHI	Information that is not encrypted while at rest or during transmission or the encryption standard used to secure PHI does not meet: • National Institute of Standards and Technology (NIST) guidelines; and • Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), a federal standard used to accredit cryptographic tools or applications
User(s)	Anyone (members of the workforce, and business associates) with access to Propio electronic data. (Also known as “users.”)
Validation	Technical evaluations used for detecting vulnerabilities in the system and verifying the effectiveness of controls to prevent security breaches.
Vendor	As it pertains to the supply chain and vendor management, it is an enterprise (or third-party) that contributes goods or services to Propio. Members of Propio’s workforce (contractors) are not considered to be vendors.
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that can be exploited by a threat.
Vulnerability Scanning	An active test run on systems or devices connected to a network to check the current configurations of systems against publicly known vulnerabilities and gauging the level of exposure and determining the overall effectiveness of the current controls.
Workforce (or Workforce Members)	Includes employees, contractors and other individuals who have an association with Propio and whose conduct, in the performance of work for Propio is under the direct control of Propio whether paid or not by Propio.

Appendix G – Training Education and Awareness Plan

	Type of Training								
Target Audience	**New hire orientation[2]**	**Phishing Training and Testing**	**Refresher Training[3]**	**Risk Analysis and Management**	**Incident Response**	**Disaster Recovery**	**InfoSec – Policies & Procedures**	**Credit card handling**	**Other _____**
New employees	**1, 4**								
All other workforce members			**3**						
Contractors or 3rd parties (not officially part of the workforce)									
All employees		**5**	**3**						
Telecommuters									
Managers				**1**	**1**				
Workforce members that handle credit cards								**1**	
IS staff and system administrators of departmental systems				**1**	**2**	**2**	**1**		

Delivery Method – Key:

1) Instructor-led "in service" or departmental meeting
2) Traditional classroom training with hands-on activities
3) Annual online computer based training *(Example: HealthStream or NetLearning)*
4) Training video
5) Other

Date reviewed: _____ Date updated: _____ Approved by: _____

Type of Training	Objectives (in general)
New hire orientation	• What is confidential information and protected health information (PHI) • How confidential information should be handled, stored, and destroyed • What is required to release information

2 New hire orientation covers an overview to HIPAA Privacy, patient confidentiality and information security basics

3 Annually, each employee completes their educational training requirements which include information security

	• Identification of incidents and breaches and how to report
Awareness handout	• What is confidential information and protected health information (PHI) • How to request access privileges • How to create and protect passwords • When to log off of workstations • What are the rules for working from home • When is personal use of computers allowed • What would be considered inappropriate activity, including the Internet • What the rules for using email • When can an individual be fined • Why does the organization conduct auditing and monitoring • How to report information security incidents • Who is responsible for making backups • How to protect media • What are the rules for using mobile computing devices • What are the rules for installing software on organizationally-owned computers
Phishing Training and Testing	• KnowBe4 Phishing Testing Campaign – delivered every 2 weeks • Specific threat alerts from IT
Refresher Training	• What are the new or current threats • Reminders of how should users protect and manage their passwords • What do users need to do to continually protect information resources from malicious code
Risk Analysis and Management	• What is risk analysis • How is a risk analysis conducted • How is a risk analysis documented
Incident Response	• What are the systematic steps that need to be taken when an incident is reported • How is an investigation conducted • What are the responsibilities of an incident response team • How are incidents categorized
Disaster Recovery	• What is a disaster and how is a disaster declared • What are the systematic steps that need to be taken to recovery the Data Center(s) and return to normal business operations
InfoSec – Policies & Procedures	• What are the expectations for staff that are responsible for information resources • What are the contents of the information security policies, standards, or security handbook
Credit card handling	• What are the expectations for staff that handle or process credit card transactions • How is credit card data protected

Appendix H – Cross Reference of the IS Security Manual to NIST Cybersecurity Framework

Key: ID = Identify; PR = Protect; DE = Detect; RS = Respond; RC = Recover

	IS Security Manual Chapter Title	NIST Function Subcategory Identifier	NIST CSF Function and Category
1	**Introduction**		Not Addressed
2	**Responsibilities**	ID.AM-6 ID.GV-2, 3 PR.AT-2, 4, 5 DE.DP-1 RS.CO-1	Asset Management (ID.AM) Governance (ID.GV) Awareness and Training (PR.AT) Detection Processes (DE.DP) Communications (RS.CO)
3	**Security Training, Education, and Awareness**	ID.GV-3 ID.RA-3 PR.AT-1, 2, 4, 5 PR.PT-1 DE.AE-3 DE.CM-1, 3, 4, 5, 7 RS.CO-2, 3 RS.AN-1	Governance (ID.GV) Risk Assessment (ID.RA) Awareness and Training (PR.AT) Protective Technology (PR.PT) Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Communications (RS.CO) Analysis (RS.AN)
4	**Risk Analysis and Management**	ID.AM-1, 2, 3 ID.BE-1, 2, 5 ID.GV-1, 2, 3, 4 ID.RA-1, 3, 4, 5, 6 ID.RM-1, 2, 3 PR.AC-2 PR.IP-2, 12 PR.DS-3 DE.CM-8 DE.DP-2 RS.AN-1 RS.MI-3	Asset Management (ID.AM) Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Risk Management Strategy (ID.RM) Identity Mgt, Authentication, and Access Control (PR.AC) Information Protection Processes and Procedures (PR.IP) Data Security (PR.DS) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP) Analysis (RS.AN) Mitigation (RS.MI)
5	**Access Control**	ID.AM-3, 6 ID.BE-1, 2 ID.GV-2, 3 ID.RA-1, 3 PR.AC-1, 2, 4, 5 PR.AT-2, 4, 5 PR.DS-1 PR.IP-11 PR.MA-1, 2 PR.PT-2, 3, 4 DE.CM-3 DE.DP-1	Asset Management (ID.AM) Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Identity Mgt, Authentication and Access Control (PR.AC) Awareness and Training (PR.AT) Data Security (PR.DS) Information Protection Processes and Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP)

	IS Security Manual Chapter Title	NIST Function Subcategory Identifier	NIST CSF Function and Category
6	**Remote Access**	ID.AM-4, 6 ID.GV-2, 3, 4 ID.RA-3 PR.AC-3, 5 PR.AT-3 PR.DS-1, 2 PR.MA-2 PR.PT-4 DE.CM-1, 3	Asset Management (ID.AM) Governance (ID.GV) Risk Assessment (ID.RA) Identity Mgt, Authentication and Access Control (PR.AC) Awareness and Training (PR.AT) Data Security (PR.DS) Maintenance (PR.MA) Protective Technology (PR.PT) Security Continuous Monitoring (DE.CM)
7	**Security Monitoring and Auditing**	ID.GV-3, 4 ID.RA-3, 5 PR.AC-5 PR.DS-1 PR.MA-2 PR.PT-1, 2, 4 DE.AE-1, 3 DE.CM-1, 3, 4, 5, 6, 7 RS.AN-1	Governance (ID.GV) Risk Assessment (ID.RA) Identity Mgt, Authentication and Access Control (PR.AC) Data Security (PR.DS) Maintenance (PR.MA) Protective Technology (PR.PT) Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Analysis (RS.AN)
8	**Security Incident Response Procedures**	ID.BE-5 ID.GV-3 ID.RA-4 ID.RM-3 PR.IP-8, 9 DE.AE-2, 3, 4, 5 DE.DP-4 RS.RP-1 RS.CO-1, 2, 3, 4, 5 RS.AN-1, 2, 3, 4 RS.MI-1, 2, 3 RC.CO-1, 2, 3	Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Risk Management Strategy (ID.RM) Information Protection Processes and Procedures (PR.IP) Anomalies and Events (DE.AE) Detection Processes (DE.DP) Response Planning (RS.RP) Communications (RS.CO) Analysis (RS.AN) Mitigation (RS.MI) Communications (RC.CO)
9	**Business Continuity and Disaster Recovery Planning**	ID.AM-2, 5 ID.BE-1, 2, 3, 4, 5 ID.GV-3 ID.RA-1, 4, 5 ID.RM-3 PR.AC-2 PR.IP-1, 4, 5, 7, 9, 10 RS.RP-1 RS.CO-1, 4 RS.AN-2 RS.IM-1, 2 RC.RP-1 RC.IM-1, 2 RC.CO-3	Asset Management (ID.AM) Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Risk Management Strategy (ID.RM) Identity Mgt, Authentication and Access Control (PR.AC) Information Protection Processes and Procedures (PR.IP) Response Planning (RS.RP) Communications (RS.CO) Analysis (RS.AN) Improvements (RS.IM) Recovery Planning (RC.RP) Improvements (RC.IM) Communications (RC.CO)

	IS Security Manual Chapter Title	NIST Function Subcategory Identifier	NIST CSF Function and Category
10	**Physical Security**	ID.AM-1 ID.BE-1, 2, 3, 4, 5 ID.GV-3 ID.RA-1, 3 ID.RM-3 PR.AC-2, 4, 5 PR.DS-3 PR.IP-4, 5, 9 PR.MA-1 PR.PT-1, 3 DE.CM-2, 7 DE.DP-1 RS.RP-1 RS.CO-1, 4 RC.RP-1 RC.CO-3	Asset Management (ID.AM) Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Risk Management Strategy (ID.RM) Identity Mgt, Authentication and Access Control (PR.AC) Data Security (PR.DS) Information Protection Processes and Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP) Response Planning (RS.RP) Communications (RS.CO) Recovery Planning (RC.RP) Communications (RC.CO)
11	**Device and Media Controls**	ID.AM-1, 3 ID.GV-3 ID.RA-1, 3 PR.AC-2, 3, 4, 5 PR.DS-1, 3	Asset Management (ID.AM) Governance (ID.GV) Risk Assessment (ID.RA) Identity Mgt, Authentication and Access Control (PR.AC) Data Security (PR.DS)
11	**Device and Media Controls (cont.)**	PR.IP-5, 6 PR.MA-2 PR.PT-2, 3, 4 DE.CM-7 DE.DP-1	Information Protection Processes and Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP)
12	**Network Security**	ID.GV-3 ID.RA-3 PR.AC-3, 5 PR.DS-2 PR.MA-2 PR.PT-4 DE.CM-1, 3	Governance (ID.GV) Risk Assessment (ID.RA) Identity Mgt, Authentication and Access Control (PR.AC) Data Security (PR.DS) Maintenance (PR.MA) Protective Technology (PR.PT) Security Continuous Monitoring (DE.CM)
13	**Security Architecture**	ID.AM-1, 3 ID.GV-1, 2, 3, 4 ID.RA-3, 4 PR.AC-2, 5 PR.DS-1, 3 PR.IP-2, 4, 5, 12 PR.MA-2 PR.PT-1, 2 DE.AE-3 DE.CM-7, 8 DE.DP-2 RS.AN-1	Asset Management (ID.AM) Governance (ID.GV) Risk Assessment (ID.RA) Identity Mgt, Authentication and Access Control (PR.AC) Data Security (PR.DS) Information Protection Processes and Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT) Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP) Analysis (RS.AN)
14	**Change Control**	ID.AM-6 ID.GV-1 PR.IP-1, 3 PR.DS-6, 7 PR.AC-4 PR.MA-1, 2	Asset Management (ID.AM) Governance (ID.GV) Information Protection Processes and Procedures (PR.IP) Data Security (PR.DS) Identity Mgt, Authentication, and Access Control (PR.AC) Maintenance (PR.MA)

	IS Security Manual Chapter Title	NIST Function Subcategory Identifier	NIST CSF Function and Category
15	**Configuration Management**	ID.AM-6 ID.GV-1 PR.IP-1, 3 PR.DS-6 PR.MA-1, 2	Asset Management (ID.AM) Governance (ID.GV) Information Protection Processes and Procedures (PR.IP) Data Security (PR.DS) Maintenance (PR.MA)
16	**Security Evaluation**	ID.AM-3 ID.BE-1, 2, 5 ID.GV-3, 4 ID.RA-1, 3, 4, 5 PR.DS-1, 6 PR.IP-1, 3, 7 PR.MA-2 PR.PT-1, 4 DE.AE-1, 3 DE.CM-1, 3, 4, 5, 6, 7, 8 DE.DP-2, 5 RS.AN-1 RS.IM-1, 2	Asset Management (ID.AM) Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Data Security (PR.DS) Information Protection Processes and Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT) Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP) Analysis (RS.AN) Improvements (RS.IM)
17	**Exceptions for Noncompliance**		Not Addressed
18	**System Life Cycle Planning**	PR.IP-1, 2, 3 PR.DS-4 DE.AE-1	Information Protection Processes and Procedures (PR.IP) Data Security (PR.DS)

Appendix I– Cross Reference of the IS Security Manual to PCI DSS 3.2

	IS Security Manual Chapter Title	PCI Requirement	Brief Description
1	**Introduction**	None	
2	**Responsibilities**	12.4, 12.4.1, 12.5, 12.5.1, 12.5.2, 12.5.3, 12.5.4, 12.5.5	Assign to an individual or team with security management responsibilities
3	**Security Training, Education, and Awareness**	8.4, 12.6, 12.6.1, 12.6.2	Implement a formal security awareness program Educate employees upon hire and at least annually Require employees to acknowledge at least annually that they have read the company's security policy
4	**Risk Analysis and Management**	12.2	Establish an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment
5	**Access Control**	6.3.1, 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.2, 8.1, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5,8.1.6, 8.1.7, 8.1.8, 8.2, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.2.5, 8.2.6, 8.4, 8.5, 8.5.1, 8.6, 8.7, 8.8, 10.1	Establish procedures for creating unique user IDs and maintaining appropriate access to systems Establish rules for strong passwords Control access to two-factor authentication mechanisms Control access to databases
6	**Remote Access**	8.3, 8.1.5, 8.6, 12.3.8, 12.3.9, 12.3.10	Require two-factor authentication for remote access Define activation of remote access technologies Implement auto logoff Define activation of vendor access, limited to when needed
7	**Security Monitoring and Auditing**	10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9	Implement audit trails that capture sufficient information to determine what events occurred and by whom Define how audit logs are maintained, secured and retained
8	**Security Incident Response Procedures**	11.1.2, 12.5.3, 12.10	Create an incident response plan and distribute the plan; include response procedures for unauthorized wireless access points
9	**Business Continuity and Disaster Recovery Planning**	12.10.1	Create an incident response plan that includes business recovery and continuity procedures
10	**Physical Security**	9.1, 9.2, 9.3, 9.4, 9.5, 9.9, 9.10	Maintain physical security of the environment where credit card data is processed and stored
11	**Device and Media Controls**	9.5, 9.6, 9.7, 9.8, 9.9, 9.10	Implement device and media controls
12	**Network Security**	1.1, 1.2, 1.3, 1.5, 4.1, 4.2, 4.3, 7.2, 8.3, 8.6, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6	Maintain a secure network including wireless networks Encrypt transmission of data across open, public networks Network segmentation
13	**Security Architecture**	2.1, 2.2, 2.3, 2.4, 2.5, 3.5, 3.6, 7.2, 10.4, 11.5, 11.6	Develop configuration standards for all system components Protect cryptographic keys Maintain an inventory of in-scope systems Synchronize all critical system clocks and times Deploy file integrity monitoring
14	**Change Control**	6.4	Follow change control procedures
15	**Configuration Management**	6.2, 6.4.5, 6.4.6	Implement patch management
16	**Security Evaluation**	11.1, 11.2, 11.3, 12.11	Conduct quarterly vulnerability scans and annual penetration tests; test for wireless access points
17	**Exceptions for Noncompliance**	None	
18	**System Life Cycle Planning**	6.3, 6.5	Develop software applications based on PCI and industry best practices and incorporate throughout the life cycle

Appendix J – Cross Reference of the IS Security Manual to ISO 27001:2013

	IT Security Manual Chapter Title	ISO Standard	Brief Description
1	**Introduction**	5.1, 5.1.1, 18.1, 18.1.1, 18.2.2	Management direction for information security Policies for information security ID and compliance with legal and contractual requirements Compliance with security policies and standards
2	**Responsibilities**	5.1.2, 6.1.1, 6.1.2, 6.1.3, 6.1.4, 7.2.1, 7.2.3, 8.1, 8.1.1, 8.1.4, 12.3, 12.3.1, 12.5.1, 12.6.2, 13.1, 13.1.1, 14.2.1, 14.2.2, 14.2.3, 16.1, 16.1.1, 16.1.2, 16.1.3, 16.1.4, 16.1.5, 16.1.6, 16.1.7, 17.1, 17.1.1, 17.1.2, 17.1.3, 17.2, 17.2.1, 18.2, 18.2.1, 18.2.3	Roles and responsibilities for: • Segregation of duties • Incident response • Collection of evidence • Backup and restore • Disaster recovery and business continuity • Facilities • Evaluation • Inventory • Change management • Event reporting
3	**Security Training, Education, and Awareness**	7.2.2, 12.2, 12.2.1, 18.2.2	Information security awareness, education and training Compliance with security policies and standards
4	**Risk Analysis and Management**	12.2, 12.2.1, 18.2, 18.2.1	Information security reviews Independent review of information security Protection and controls against threats
5	**Access Control**	7.1, 7.1.1, 7.1.2, 7.3, 7.3.1, 9.1, 9.1.1, 9.1.2, 9.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.6, 9.3.1, 9.4, 9.4.2, 9.4.3, 10.1, 10.1.1, 10.1.2, 11.2.8, 13.2.3	Prior to employment screening, terms and conditions Access control policy and requirements Business requirements of access control for networks, systems, applications, email and services Termination and change of employment User access management, provisioning and deprovisioning Privileged access rights Authentication, passwords and password management systems Encryption and key management Unattended user equipment
6	**Remote Access**	7.3, 7.3.1, 8.1.4, 9.2, 9.2.1, 9.2.2, 9.4.3, 15.1, 15.1.1, 15.1.2, 15.1.3	Remote user access management (provisioning/deprovisioning) Teleworking, termination and change of employments Return of assets Two-factor authentication Information security policy for supplier relationships Supply chain security
7	**Security Monitoring and Auditing**	8.1.1, 9.2.5, 12.4, 12.4.1, 12.4.2, 12.7, 12.7.1, 18.2.1, 18.2.3	Information systems audit considerations and controls Event logging, and monitoring, and log protection Review of user access rights Independent review of information security Technical compliance review
8	**Security Incident Response Procedures**	6.1.3, 12.2, 12.2.1, 16.1, 16.1.1, 16.1.2, 16.1.3, 16.1.4, 16.1.5, 16.1.6, 16.1.7	Management of security incidents and improvements Responsibilities and procedures Reporting information security events and weaknesses Response to information security incidents Learning from information security incidents Collection of evidence
9	**Business Continuity and Disaster Recovery Planning**	12.2, 12.2.1, 12.3, 12.3.1, 17.1, 17.1.1,	Backup and restore Planning, implementing, verifying, and evaluating continuity

	IT Security Manual Chapter Title	ISO Standard	Brief Description
		17.1.2, 17.1.3, 17.2.1, 17.2	Availability of information processing facilities Resiliency
10	**Physical Security**	11.1, 11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.5, 11.1.6, 11.2.2, 11.2.4, 11.2.5, 11.2.7	Secure areas and physical security perimeters Physical entry controls Securing offices, rooms and facilities Protecting against external end environmental threats Supporting utilities Equipment maintenance Removal disposal and re-use of equipment
11	**Device and Media Controls**	6.2, 6.2.1, 8.3, 8.3.1, 8.3.2, 8.3.3, 10.1, 10.1.1, 10.1.2, 11.2.5, 11.2.7, 12.5.1, 12.6.2, 13.2.3	Mobile device policy Media and removable media handling (removal, re-use, and disposal) Encryption and key management Restrictions on software installation Electronic messaging
12	**Network Security**	12.2, 12.2.1, 13.1, 13.1.1, 13.1.2, 13.1.3, 13.2.3, 14.1, 14.1.2, 14.1.3, 14.2.5	Secure system engineering and network services principles Security requirements of information systems Securing applications services on public networks Network controls and network security management Network segregation Protection from malware Electronic messaging Protecting application services transactions
13	**Security Architecture**	7.3, 7.3.1, 8.1.1, 10.1, 10.1.1, 10.1.2, 12.1.4, 12.2, 12.2.1, 12.4, 12.4.1, 12.4.2, 12.4.4, 13.1, 14.1, 14.2.5	Secure architecture principles Security requirements of information systems Inventory of assets Secure architecture for access control, encryption, key management Network security management Separation of development, testing and operational environments Malware protection Logging, monitoring, and protection of log information Clock synchronization
14	**Change Control**	12.1.2, 12.1.3, 14.2.2, 14.2.3, 14.2.4	Change management Capacity management System change control procedures Technical review of applications after platform changes Restrictions on changes to software packages
15	**Configuration Management**	13.2.3, 14.1	Security requirements of information systems Electronic messaging
16	**Security Evaluation**	12.6, 12.6.1, 14.2.8, 14.2.9, 18.2.3	Technical vulnerability management System security testing System acceptance testing Technical compliance review
17	**Exceptions for Noncompliance**		
18	**System Life Cycle Planning**	6.1.5, 12.6, 12.6.1, 14.1, 14.2, 14.2.1, 14.2.8, 14.2.9, 14.2.3	Security requirements of information systems Information security in project management Security in development and support processes Secure development policy System security and acceptance testing Technical review of applications after platform changes Technical vulnerability management

Appendix K – Cross Reference of the IS Security Manual to CIS Top-20

	IS Security Manual Chapter Title	CIS Top-20 Requirement	Brief Description
1	**Introduction**		Not Addressed
2	**Responsibilities**	1.4, 2.1, 3.1, 6.7, 9.3, 10.1, 10.2, 10.3, 10.4, 11.1, 11.3, 12.1, 12.7, 15.4, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9, 18.5, 18.6, 19.1, 19.2, 19.3, 19.6, 19.7, 20.1, 20.2	1. Inventory and Control of Hardware Assets 2. Inventory and Control of Software Assets 3. Continuous Vulnerability Management 6. Maintenance, Monitoring and Analysis of Logs 9. Control of Network Ports, Services and Protocols 10. Disaster Recovery 11. Control of Network Device Configuration 12. Perimeter Defense 15. Wireless Access Control 17. Security Awareness and Training 18. Application Software Security 19. Incident Response and Management 20. Penetration Testing and Red Team Exercises
3	**Security Training, Education, and Awareness**	8.1, 8.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9, 18.6, 19.6	8. Malware Defenses 17. Security Awareness and Training 18. Application Software Security 19. Incident Response and Management
4	**Risk Analysis and Management**	1.4, 2.1, 3.1, 3.7, 9.3, 13.1	1. Inventory and Control of Hardware Assets 2. Inventory and Control of Software Assets 3. Continuous Vulnerability Management 9. Control of Network Ports, Services and Protocols
5	**Access Control**	4.4, 4.5, 10.1, 10.4, 12.11, 13.6, 13.9, 14.4, 14.6, 14.8, 16.3, 16.7, 16.8, 16.9, 16.11, 18.5	4. Controlled Use of Administrative Privileges 10. Disaster Recovery 12. Perimeter Defense 13. Data Protection 14. Configuration Based on Need to Know 16. Account Monitoring and Control 18. Application Software Security
6	**Remote Access**	4.5, 12.11, 16.3, 16.7, 16.11	4. Controlled Use of Administrative Privileges 12. Perimeter Defense 16. Account Monitoring and Control
7	**Security Monitoring and Auditing**	2.6, 3.1, 6.2, 6.6, 6.7, 14.9, 16.12	2. Inventory and Control of Software Assets 3. Continuous Vulnerability Management 6. Maintenance, Monitoring and Analysis of Logs 14. Configuration Based on Need to Know 16. Account Monitoring and Control
8	**Security Incident Response Procedures**	8.1, 8.2, 9.3, 19.1, 19.2, 19.3, 19.6, 19.7	8. Malware Defenses 9. Control of Network Ports, Services and Protocols 19. Incident Response and Management
9	**Business Continuity and Disaster Recovery Planning**	1.4, 2.1, 10.1, 10.2, 10.3, 10.4, 13.1	1. Inventory and Control of Hardware Assets 2. Inventory and Control of Software Assets 10. Disaster Recovery 13. Data Protection
10	**Physical Security**		Not Addressed

	IS Security Manual Chapter Title	CIS Top-20 Requirement	Brief Description
11	**Device and Media Controls**	1.4, 2.1, 2.6, 3.4, 5.1, 7.4, 7.9, 8.1, 8.2, 10.1, 13.6, 13.7, 13.9, 14.4, 14.8, 16.11	1. Inventory and Control of Hardware Assets 2. Inventory and Control of Software Assets 3. Continuous Vulnerability Management 5. Secure Configuration of Hardware and Software 7. Email and Web Browser Protections 8. Malware Defenses 10. Disaster Recovery 13. Data Protection 14. Configuration Based on Need to Know 16. Account Monitoring and Control
12	**Network Security**	5.1, 6.7, 7.4, 9.2, 11.3, 12.1, 12.7, 14.1, 14.4, 14.8, 15.4, 15.7, 15.10	5. Secure Configuration of Hardware and Software 6. Maintenance, Monitoring and Analysis of Logs 7. Email and Web Browser Protections 9. Control of Network Ports, Services and Protocols 11. Control of Network Device Configuration 12. Perimeter Defense 14. Configuration Based on Need to Know 15. Wireless Access Control
13	**Security Architecture**	1.4, 2.1, 3.4, 5.1, 8.1, 8.2, 9.2, 10.1, 13.6, 14.4, 14.8, 18.9	1. Inventory and Control of Hardware Assets 2. Inventory and Control of Software Assets 3. Continuous Vulnerability Management 5. Secure Configuration of Hardware and Software 8. Malware Defenses 9. Control of Network Ports, Services and Protocols 10. Disaster Recovery 13. Data Protection 14. Configuration Based on Need to Know 18. Application Software Security
14	**Change Control**		Not addressed
15	**Configuration Management**	3.1, 3.4, 5.1, 5.4, 9.3	3. Continuous Vulnerability Management 5. Secure Configuration of Hardware and Software 9. Control of Network Ports, Services and Protocols
16	**Security Evaluation**	20.1, 20.2	20. Penetration Testing and Red Team Exercises
17	**Exceptions for Noncompliance**		Not Addressed
18	**System Life Cycle Planning**	3.1, 9.3, 10.1, 18.1	3. Continuous Vulnerability Management 9. Control of Network Ports, Services and Protocols 10. Disaster Recovery 18. Application Software Security

Note: *Some CIS controls do not appear in the cross reference table because they are either subsets of other controls or are controls not commonly implemented in healthcare due to impracticality*

Appendix L – Cross Reference of the IS Security Manual to HITRUST 9.1

	IS Security Manual Chapter Title	HITRUST Requirement	Brief Description
1	**Introduction**	00.a, 03.a, 04.a, 04.b, 05.a, 05.b, 05.c, 06.a, 06.d, 08.d, 09.a, 09.q	• Information Security Management Program • Risk Management Program Development • Information Security Policy Document • Review of the Information Security Policy • Management Commitment to Information Security • Information Security Coordination • Allocation of Information Security Responsibilities • Identification of Applicable Legislation • Data Protection and Privacy of Covered Information • Protecting Against External and Environmental Threats • Documented Operations Procedures • Information Handling Procedures
2	**Responsibilities**	00.a, 01.e, 01.k, 01.l, 01.s, 01.v, 02.a, 02.e, 02.f, 02.g, 02.i, 03.a, 03.b, 03.c, 03.d, 04.a, 04.b, 05.a, 05.b, 05.c, 05.d, 05.f, 05.g, 05.i, 05.k, 06.b, 06.d, 06.e, 06.g, 06.h, 06.i, 07.a, 07.b, 08.a, 08.b, 08.c, 08.d, 08.e, 08.f, 08.g, 08.h, 08.k, 08.l, 08.m, 09.a, 09.ab, 09.ad, 09.ae, 9.c, 09.e, 09.f, 09.g, 09.h, 09.i, 09.l, 09.m, 09.n, 09.t, 09.u, 09.v, 09.x, 09.y, 10.a, 10.b, 10.c, 10.d, 10.e, 10.i, 10.k, 10.m, 11.a, 11.b, 11.c, 11.d, 11.e, 12.a, 12.b, 12.c, 12.d, 12.e	• Information Security Management Program • Review of User Access Rights • Equipment Identification in Networks • Remote Diagnostic and Configuration Port Protection • Use of System Utilities • Information Access Restriction • Roles and Responsibilities • Information Security Awareness, Education, and Training • Disciplinary Process • Termination or Change Responsibilities • Removal of Access Rights • Risk Management Program Development • Performing Risk Assessments • Risk Mitigation • Risk Evaluation • Information Security Policy Document • Review of the Information Security Policy • Management Commitment to Information Security • Information Security Coordination • Allocation of Information Security Responsibilities • Authorization Process for Information Assets and Facilities • Contact with Authorities • Contact with Special Interest Groups • Identification of Risks Related to External Parties • Addressing Security in Third Party Agreements • Intellectual Property Rights • Data Protection and Privacy of Covered Information • Prevention of Misuse of Information Assets • Compliance with Security Policies and Standards • Technical Compliance Checking • Information Systems Audit Controls • Inventory of Assets • Ownership of Assets • Physical Security Perimeter • Physical Entry Controls • Securing Offices, Rooms, and Facilities • Protecting Against External and Environmental Threats • Working in Secure Areas • Public Access, Delivery, and Loading Areas • Equipment Siting and Protection

	IS Security Manual Chapter Title	HITRUST Requirement	Brief Description
	Responsibilities (continued)		• Supporting Utilities • Security of Equipment Off-Premises • Secure Disposal or Re-Use of Equipment • Removal of Property • Documented Operations Procedures • Monitoring System Use • Administrator and Operator Logs • Fault Logging • Segregation of Duties • Service Delivery • Monitoring and Review of Third Party Services • Managing Changes to Third Party Services • Capacity Management • System Acceptance • Back-up • Network Controls • Security of Network Services • Exchange Agreements • Physical Media in Transit • Electronic Messaging • Electronic Commerce Services • On-line Transactions • Security Requirements Analysis and Specification • Input Data Validation • Control of Internal Processing • Message Integrity • Output Data Validation • Protection of System Test Data • Change Control Procedures • Control of Technical Vulnerabilities • Reporting Information Security Events • Reporting Security Weaknesses • Responsibilities and Procedures • Learning from Information Security Incidents • Collection of Evidence • Including Information Security in the Business Continuity Management Process • Business Continuity and Risk Assessment • Developing and Implementing Continuity Plans Including Information Security • Business Continuity Planning Framework • Testing, Maintaining and Re-Assessing Business Continuity Plans
3	**Security Training, Education, and Awareness**	01.g, 02.e, 03.a, 04.a, 06.b, 06.c, 08.g, 08.k, 08.l, 09.a, 09.j, 09.o, 09.p, 09.q, 09.u, 11.a, 11.b, 11.c	• Unattended User Equipment • Information Security Awareness, Education, and Training • Risk Management Program Development • Information Security Policy Document • Intellectual Property Rights • Protection of Organizational Records • Equipment Siting and Protection • Security of Equipment Off-Premises • Secure Disposal or Re-Use of Equipment • Documented Operations Procedures • Controls Against Malicious Code

	IS Security Manual Chapter Title	HITRUST Requirement	Brief Description
	Security Training, Education, and Awareness (continued)		• Management of Removable Media • Disposal of Media • Information Handling Procedures • Physical Media in Transit • Reporting Information Security Events • Reporting Security Weaknesses • Responsibilities and Procedures
4	**Risk Analysis and Management**	00.a, 03.b, 03.c, 03.d, 05.a, 05.c, 06.c, 06.d, 07.a, 08.a, 08.b, 08.c, 08.d, 09.e, 09.f, 09.r, 09.v, 09.x, 09.y, 10.m, 12.a, 12.b, 12.c, 12.d, 12.e	• Information Security Management Program • Performing Risk Assessments • Risk Mitigation • Risk Evaluation • Management Commitment to Information Security • Allocation of Information Security Responsibilities • Protection of Organizational Records • Data Protection and Privacy of Covered Information • Inventory of Assets • Physical Security Perimeter • Physical Entry Controls • Securing Offices, Rooms, and Facilities • Protecting Against External and Environmental Threats • Service Delivery • Monitoring and Review of Third Party Services • Security of System Documentation • Electronic Messaging • Electronic Commerce Services • On-line Transactions • Control of Technical Vulnerabilities • Including Information Security in the Business Continuity Management Process • Business Continuity and Risk Assessment • Developing and Implementing Continuity Plans Including Information Security • Business Continuity Planning Framework • Testing, Maintaining and Re-Assessing Business Continuity Plans
5	**Access Control**	01.a, 01.b, 01.c, 01.d, 01.e, 01.f, 01.g, 01.h, 01.i, 01.n, 01.o, 01.p, 01.q, 01.r, 01.s, 01.t, 01.v, 02.b, 02.c, 02.g, 02.h, 02.i, 05.d, 05.e, 06.e, 06.f, 06.i, 08.m, 09.l, 09.r, 09.v, 09.x, 09.y, 10.f	• Access Control Policy • User Registration • Privilege Management • User Password Management • Review of User Access Rights • Password Use • Unattended User Equipment • Clear Desk and Clear Screen Policy • Policy on Use of Network Services • Network Connection Control • Network Routing Control • Secure Log-on Procedures • User Identification and Authentication • Password Management System • Use of System Utilities • Session Time-out • Information Access Restriction • Screening • Terms and Conditions of Employment

	IS Security Manual Chapter Title	HITRUST Requirement	Brief Description
	Access Control (continued)		• Termination or Change Responsibilities • Return of Assets • Removal of Access Rights • Authorization Process for Information Assets and Facilities • Confidentiality Agreements • Prevention of Misuse of Information Assets • Regulation of Cryptographic Controls • Information Systems Audit Controls • Removal of Property • Back-up • Security of System Documentation • Electronic Messaging • Electronic Commerce Services • On-line Transactions • Policy on the Use of Cryptographic Controls
6	**Remote Access**	01.a, 01.b, 01.e, 01.i, 01.j, 01.n, 01.p, 01.v, 02.a, 02.c, 02.d, 02.g, 02.i, 05.i, 05.k, 06.c, 06.d, 09.e, 09.f, 09.g, 09.m, 09.n, 09.t, 11.a, 11.b	• Access Control Policy • User Registration • Review of User Access Rights • Policy on Use of Network Services • User Authentication for External Connections • Network Connection Control • Secure Log-on Procedures • Information Access Restriction • Roles and Responsibilities • Terms and Conditions of Employment • Management Responsibilities • Termination or Change Responsibilities • Removal of Access Rights • Identification of Risks Related to External Parties • Addressing Security in Third Party Agreements • Protection of Organizational Records • Data Protection and Privacy of Covered Information • Service Delivery • Monitoring and Review of Third Party Services • Managing Changes to Third Party Services • Network Controls • Security of Network Services • Exchange Agreements • Reporting Information Security Events • Reporting Security Weaknesses
7	**Security Monitoring and Auditing**	01.e, 01.k, 03.d, 06.e, 06.i, 07.a, 09.a, 09.ad, 09.ae, 09.f, 10.m	• Review of User Access Rights • Equipment Identification in Networks • Risk Evaluation • Prevention of Misuse of Information Assets • Information Systems Audit Controls • Inventory of Assets • Monitoring System Use • Administrator and Operator Logs • Fault Logging • Monitoring and Review of Third Party Services • Control of Technical Vulnerabilities
8	**Security Incident Response Procedures**	02.f, 05.f, 05.g, 06.a, 06.b, 08.d, 11.a, 11.b, 11.c, 11.d, 11.e	• Disciplinary Process • Contact with Authorities • Contact with Special Interest Groups

	IS Security Manual Chapter Title	HITRUST Requirement	Brief Description
	Security Incident Response Procedures (continued)		• Identification of Applicable Legislation • Intellectual Property Rights • Protecting Against External and Environmental Threats • Reporting Information Security Events • Reporting Security Weaknesses • Responsibilities and Procedures • Learning from Information Security Incidents • Collection of Evidence
9	**Business Continuity and Disaster Recovery Planning**	07.a, 09.l, 10.a, 12.a, 12.b, 12.c, 12.d, 12.e	• Inventory of Assets • Back-up • Security Requirements Analysis and Specification • Including Information Security in the Business Continuity Management Process • Business Continuity and Risk Assessment • Developing and Implementing Continuity Plans Including Information Security • Business Continuity Planning Framework • Testing, Maintaining and Re-Assessing Business Continuity Plans
10	**Physical Security**	01.a, 01.g, 01.v, 01.y, 05.d, 08.a, 08.b, 08.c, 08.e, 08.f, 08.g, 08.h, 08.j 08.k, 08.l, 08.m, 09.q, 09.u	• Access Control Policy • Unattended User Equipment • Information Access Restriction • Teleworking • Authorization Process for Information Assets and Facilities • Physical Security Perimeter • Physical Entry Controls • Securing Offices, Rooms, and Facilities • Working in Secure Areas • Public Access, Delivery, and Loading Areas • Equipment Siting and Protection • Supporting Utilities • Equipment Maintenance • Security of Equipment Off-Premises • Secure Disposal or Re-Use of Equipment • Removal of Property • Information Handling Procedures • Physical Media in Transit
11	**Device and Media Controls**	01.h, 01.s, 01.t, 01.x, 01.y, 03.c, 06.a, 06.c, 06.e, 06.f, 08.g, 08.k, 08.l 08.m, 09.j, 09.k, 09.l, 09.o, 09.p, 09.q, 09.r, 09.u, 09.v, 09.x, 09.y, 10.a, 10.f, 10.g	• Clear Desk and Clear Screen Policy • Use of System Utilities • Session Time-out • Mobile Computing and Communications • Teleworking • Risk Mitigation • Identification of Applicable Legislation • Protection of Organizational Records • Prevention of Misuse of Information Assets • Regulation of Cryptographic Controls • Equipment Siting and Protection • Security of Equipment Off-Premises • Secure Disposal or Re-Use of Equipment • Removal of Property • Controls Against Malicious Code • Controls Against Mobile Code • Back-up

	IS Security Manual Chapter Title	HITRUST Requirement	Brief Description
	Device and Media Controls (continued)		• Management of Removable Media • Disposal of Media • Information Handling Procedures • Security of System Documentation • Physical Media in Transit • Electronic Messaging • Electronic Commerce Services • On-line Transactions • Security Requirements Analysis and Specification • Policy on the Use of Cryptographic Controls • Key Management
12	**Network Security**	01.a, 01.i, 01.l, 01.m, 01.n, 01.o, 01.t, 01.w, 01.x, 06.f, 06.i, 09.m, 09.v, 09.x, 09.y, 10.b, 10.c, 10.d, 10.e, 10.f	• Access Control Policy • Policy on Use of Network Services • Remote Diagnostic and Configuration Port Protection • Segregation in Networks • Network Connection Control • Network Routing Control • Session Time-out • Sensitive System Isolation • Mobile Computing and Communications • Regulation of Cryptographic Controls • Information Systems Audit Controls • Network Controls • Electronic Messaging • Electronic Commerce Services • On-line Transactions • Input Data Validation • Control of Internal Processing • Message Integrity • Output Data Validation • Policy on the Use of Cryptographic Controls
13	**Security Architecture**	01.a, 01.c, 01.l, 01.m, 01.p, 01.t, 01.w, 02.g, 02.h, 02.i, 03.c, 06.e, 06.f, 06.i, 07.a, 08.d, 09.af, 09.c, 09.d, 09.j, 09.l, 09.m, 09.v, 09.x, 09.y, 10.b, 10.c, 10.d, 10.e, 10.f, 10.g, 10.i	• Access Control Policy • Privilege Management • Remote Diagnostic and Configuration Port Protection • Segregation in Networks • Secure Log-on Procedures • Session Time-out • Sensitive System Isolation • Termination or Change Responsibilities • Return of Assets • Removal of Access Rights • Risk Mitigation • Prevention of Misuse of Information Assets • Regulation of Cryptographic Controls • Information Systems Audit Controls • Inventory of Assets • Protecting Against External and Environmental Threats • Clock Synchronization • Segregation of Duties • Separation of Development, Test, and Operational Environments • Controls Against Malicious Code • Back-up • Network Controls

	IS Security Manual Chapter Title	HITRUST Requirement	Brief Description
	Security Architecture (continued)		• Electronic Messaging • Electronic Commerce Services • On-line Transactions • Input Data Validation • Control of Internal Processing • Message Integrity • Output Data Validation • Policy on the Use of Cryptographic Controls • Key Management • Protection of System Test Data
14	**Change Control**	08.j, 09.b, 09.h, 09.i, 10.k	• Equipment Maintenance • Change Management • Capacity Management • System Acceptance • Change Control Procedures
15	**Configuration Management**	01.l, 01.p, 06.h, 10.m	• Remote Diagnostic and Configuration Port Protection • Secure Log-on Procedures • Technical Compliance Checking • Control of Technical Vulnerabilities
16	**Security Evaluation**	05.h	• Independent Review of Information Security
17	**Exceptions for Noncompliance**		• Not Addressed
18	**System Life Cycle Planning**	03.c, 03.d, 06.c, 06.f, 06.h, 08.j, 08.k, 08.l, 10.a, 10.f, 10.m, 12.a, 12.b, 12.c, 12.d, 12.e	• Risk Mitigation • Risk Evaluation • Protection of Organizational Records • Regulation of Cryptographic Controls • Technical Compliance Checking • Equipment Maintenance • Security of Equipment Off-Premises • Secure Disposal or Re-Use of Equipment • Security Requirements Analysis and Specification • Policy on the Use of Cryptographic Controls • Control of Technical Vulnerabilities • Including Information Security in the Business Continuity Management Process • Business Continuity and Risk Assessment • Developing and Implementing Continuity Plans Including Information Security • Business Continuity Planning Framework • Testing, Maintaining and Re-Assessing Business Continuity Plans