Contents

1 Introduction 3
- 1.1 ISO 27001:2022 3
- 1.2 Plan-Do-Check-Act (PDCA) cycle 4

2 References 4

3 Terms and Definitions 4

4 Business Context 5
- 4.1 Understanding our organization and its context 5
- 4.2 Understanding the needs and expectations of interested parties 5
- 4.3 Scope of the Information Security Management System (ISMS) 6
  - 4.3.1 Scope 6
  - 4.3.2 Exclusions 7
- 4.4 Information Security Management System 7

5 Leadership 7
- 5.1 Leadership and Commitment 7
- 5.2 Information Security Policy 8
- 5.3 Organizational roles, responsibilities & authorities 8

6 Planning 10
  - 6.1.1 General 11
  - 6.1.2 Planning actions to achieve our Information Security Objectives 12

7 Support 13
- 7.1 Resources 13
  - 7.1.1 General 13
- 7.2 Competency, and Awareness, and Communication 13
- 7.3 Documentation and records 14
  - 7.3.1 General 14
  - 7.3.2 Control of documents 15
  - 7.3.3 Control of records 15
- 7.4 Customer Communications 15

8 Operations 15
- 8.1 Operational planning and control 15
- 8.2 Information security risk assessment 16
- 8.3 Information Security Risk Treatment 16

9 Performance Evaluation 17
9.2 Monitoring, measurement, analysis and evaluation 17
9.3 Internal audit 17
9.4 Management Review 18
10 Improvement 18
10.2 General 18
10.3 Non-conformity and corrective action 19
10.4 Continual improvement 19
10.5 Customer Complaint Management Procedure 19
11 Annex A – Control Objectives and Controls 20
12 Appendix 1 - Organization Chart 21
13 Appendix 2 - Organisational High-Level Process Map 22
Document Title: ISMS **1**

1 Introduction

Patient Partner has developed and implemented an Information Security Management System (ISMS) which enables us to:

- assess and treat information security risks following our particular needs
- demonstrate commitment and compliance to global best practice
- demonstrate to customers, suppliers, and stakeholders that security is paramount to the way we operate
- better secure all financial and confidential data, so minimizing the likelihood of it being accessed illegally or without permission

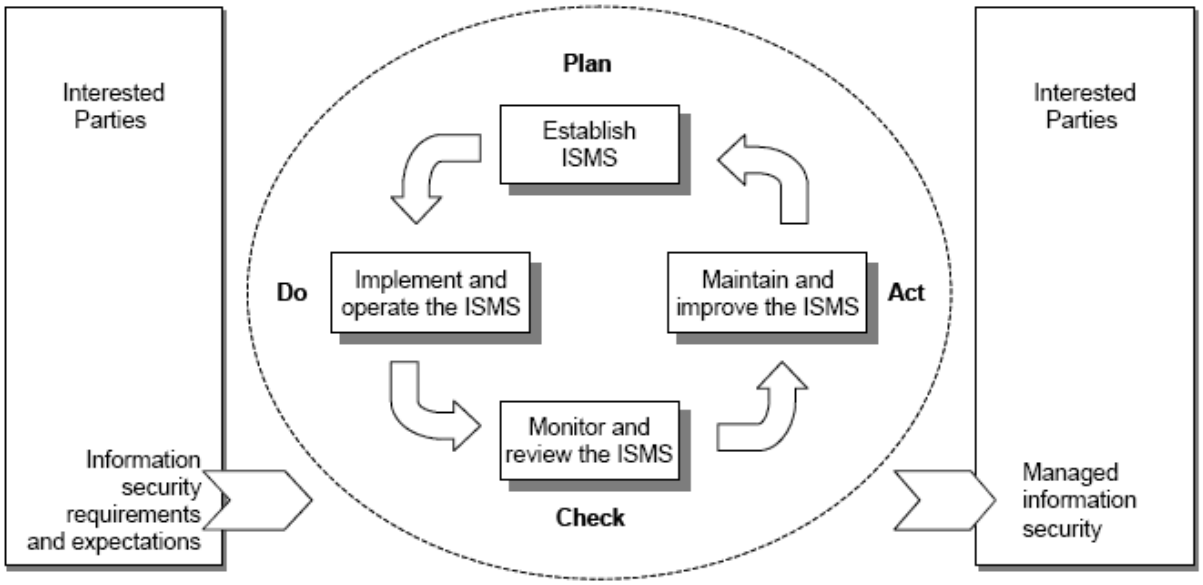
This manual describes our ISMS and sets out the authorities and responsibilities of those operating within it. It also references procedures and activities that fall within its scope.

1.1 ISO 27001:2022

Our ISMS has been developed in compliance with the ISO 27001:2022 standard, which sets out a process-based approach for establishing, implementing, maintaining, and continually improving our ISMS within the context of our organization.

The processes and the system as a whole are managed using the Plan-Do-Check-Act (PDCA) cycle, with an overall focus on using risk-based thinking to take advantage of opportunities and prevent undesirable information security results.

1.2 Plan-Do-Check-Act (PDCA) cycle



2 References

Standard	Title	Description
ISO 27001:2022	information security management Systems	Requirements
ISO 27002:2022	Information technology - security techniques	Code of practice for information security controls
ISO 9001:2015	Quality Management System	Requirements

3 Terms and Definitions

The terminology used in this ISMS reflects both that used in ISO 27001:2022 and:

- standard business/quality terminology
- terms and vocabulary typically used within our scope of activity
- terms typically used in standards and regulations as they relate to our scope of activity

Definitions:

- “Compliance obligations” means both those laws and other requirements, be they national or international, that apply to us as an organization, and any other

commitments we enter into, or apply voluntarily, such as contracts, agreements, codes, and standards

- "Top Management", as referred to by ISO, is represented in Patient Partner by the Senior Leadership Team
- "Personnel" are all those working under our control

4 Business Context

4.1 Understanding our organization and its context

4.2 Understanding the needs and expectations of interested parties

Patient Partner identifies all critical internal and external issues relevant to our operations that affect our ability to achieve the intended outcomes of our ISMS.

This involves:

- Understanding our core products/services/processes- Processes:
    - PatientPartner is a patient engagement platform that increases patient-driven adoption, conversion, and adherence for pharmaceutical and medical device brands. It is the only real-time patient engagement platform available on the market. Their technology creates meaningful connections between prospective patients and experienced patient mentors to learn from firsthand knowledge about breakthrough treatments.
- understanding the scope of our ISMS
- interested parties ("stakeholders") who are relevant to our ISMS include:
    - Customers
    - 3rd Party Vendors
    - Employees/contractors
    - Auditors
    - Partners
    - Regulatory bodies

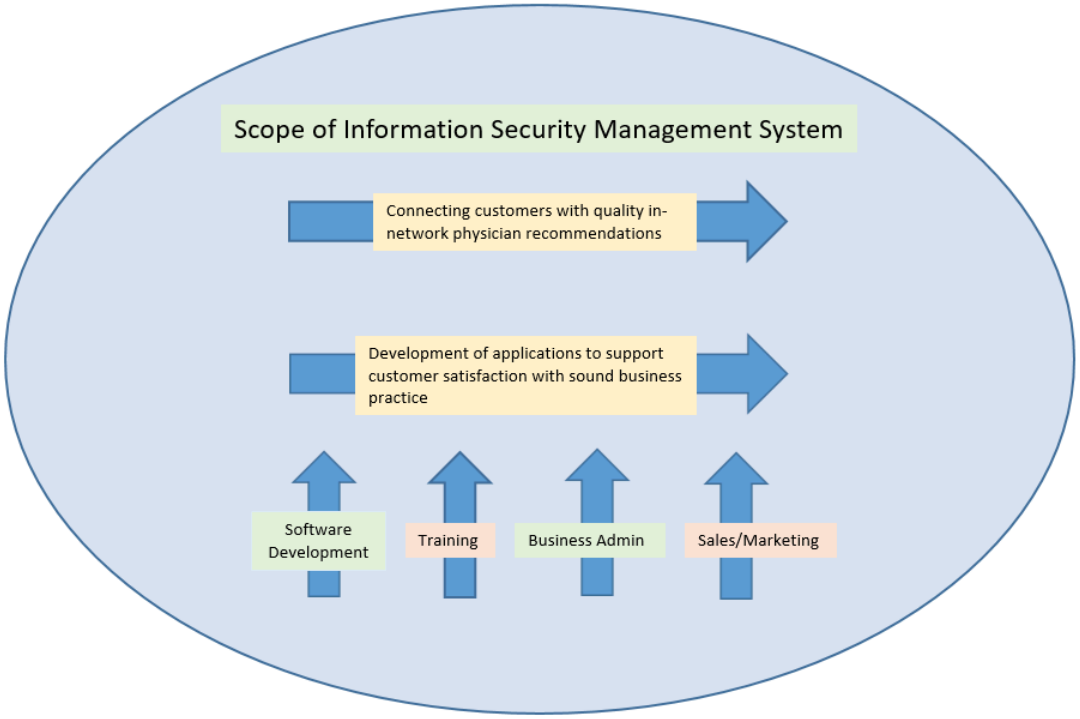
We operate and maintain our ISMS compliance with legal and contractual requirements to ensure conformance with:

- legal, statutory, regulatory, or contractual obligations related to information security

4.3 Scope of the Information Security Management System (ISMS)

4.3.1 Scope

Our information management security system satisfies the requirements of ISO 27001:2022 and, based on our understanding of our business and the needs and expectations of our stakeholders, addresses and supports our processes at our office in 1025 Prospect St, La Jolla, CA 92034 for management, administration and the design, development, and servicing of our products, including software development and maintenance.



PatientPartner's Information Security Management System (ISMS) applies to the control of our entire business, premises, and resources. Our ISMS will protect the confidentiality, integrity, and availability of our customer and business data at all times.

When determining this scope, we have considered:

- our organization and its context (both internal and external issues)
- the needs and expectations of interested parties
- the interfaces and dependencies between activities performed by ourselves and those that are performed by other organizations

4.3.2 Exclusions

The following are excluded from our ISMS as they do not apply to our business.

Exclusions	Reason for Exclusion

4.4 Information Security Management System

To achieve our Information Security Objectives, we have established, implemented, maintained, and continually improved our ISMS, including the processes needed and their interactions.

Our ISMS takes into consideration the needs and expectations of interested parties.

5 Leadership

5.1 Leadership and Commitment

The Leadership Team demonstrates leadership and commitment to achieving the objectives of our ISMS by taking accountability for the effectiveness of our ISMS and ensuring that:

- an Information Security Policy and Information Security Objectives are established for the management system, and they are compatible with our strategic direction and context
- our ISMS requirements are integrated into our business processes as appropriate
- our ISMS is suitably resourced

- there is clear communication on the importance of effective information security management and of conforming to the management system requirements
- our ISMS achieves its intended results
- all personnel are encouraged to contribute to the effectiveness of the management system
- continual improvement is actively promoted
- our information security policies, objectives, and targets are, where appropriate, reflected in individual responsibilities and performance objectives

5.2 Information Security Policy

The Leadership Team has developed our Information Security Policy, which is to:

Establish, monitor, and continually improve our safeguards for the confidentiality, integrity, and availability of all physical and electronic information assets to maintain regulatory, operational, and contractual requirements so PatientPartner can provide our service of connecting our users to past patients and top-tier care providers. Provide needed resources to support our security objectives and commit to continual improvement.

Our Information Security Policy is typically reviewed annually, as part of our information security management review meeting or as required to recognize relevant interested parties' changing needs and expectations or the risks and opportunities identified by the risk management process.

5.3 Organizational roles, responsibilities & authorities

The Leadership team has assigned responsibilities and authorities for all roles relevant to the full and proper implementation, operation, and maintenance of this management system, including the following:

Responsibility	Principal Responsible Persons
Determination of organizational context, establishment of overall direction, framing of policies for information security management, and conduct of management review	CEO
Ensuring the promotion of a focus on information security matters throughout the organization	CTO

Framing of ISMS objectives, targets, and plans	CTO
Control of ISMS documents	CTO
Control of ISMS records	CTO
Information security training, awareness, and competence	COO and CTO
Management of internal ISMS audits	CTO
Corrective and/or preventive actions (CAPA)	CTO
Assessment and treatment of information security risks	CTO and Risk Owners
Ensuring that our ISMS conforms to applicable standards	CTO
Implementation, operation, monitoring, review, maintenance, and Improvement of the ISMS	CTO
Ensuring that the integrity of our ISMS is maintained when changes are planned and implemented	CTO
Organizing of independent review of information security management practices of the company	CTO and Information Security Advisor (Contract)
Achieving and maintaining appropriate protection of organizational assets and ensuring that information receives an appropriate level of protection	CTO
Human resources security (prior to employment, during employment, and, on termination or change of employment)	COO and CTO
Physical and environmental security	COO and CTO
Communications and operations management	CTO
Media handling and information exchange	CTO
Network security management and access control	CTO
Privacy/Data Protection	CTO
Acquisition, development, and maintenance of information systems	COO, CTO
Information security incident management	CTO

Business continuity management	CTO
Complying with legal and regulatory requirements regarding information security including EU GDPR and other country, local, and Independent Ethics Committee-required privacy and data protection practices	CTO
Complying with contractual obligations regarding information security	CEO and CTO

These responsibilities and authorities are communicated through the combination of our Organization Chart and internal Job Titles.

- CEO - Link to job description & qualifications (Resume + Cover Letter)
  - Background Check
- COO - Link to job description & qualifications (Resume + Cover Letter)
  - Background Check
- CTO - Link to job description & qualifications (Resume + Cover Letter)

All managers are expected to demonstrate their commitment to the development and improvement of our ISMS through:

- the provision of necessary resources
- their proactive involvement in continual improvement activities
- focusing on the improvement of key system processes

All managers are responsible for implementing the policies, processes, and systems described in this manual within their area of responsibility.

All personnel are responsible for implementing the policies and procedures applicable to their processes. They are encouraged to identify and report any known or potential problems and recommend related solutions.

6 Planning

We have identified the risks and opportunities that need to be addressed. Those risks and opportunities have been addressed to:

- ensure that our ISMS can achieve its intended outcomes

- prevent or reduce undesirable effects
- achieve continual improvement

When managing risks and opportunities, we have defined and applied an information security risk assessment process that establishes and maintains information security risk criteria, including the risk acceptance criteria and criteria for performing information security risk assessments.

- we consider risks and opportunities when taking actions within our ISMS, as well as when implementing or improving our ISMS
- formal risk management may not be utilized in all circumstances, and the level of risk assessment, analysis, actions, and recording will be to a level appropriate to each circumstance
- the actions we take to address risks and opportunities are proportionate to the Establishing and achieving Information Security Objectives

6.1.1 General

The Leadership Team has developed our Information Security Objectives, which are to:

Measure target objective/goal	Impactful Activities	Responsible person	Resources needed	Reporting frequency
Access Control: Review access to our system once a quarter	Review access to all critical systems and remove access to any persons who no longer require access	CTO	Admin access to critical systems	Quarterly at regular management meetings
Logging and Monitoring: Review critical logs for anomalous behavior every quarter	Review logs for anomalous activity and investigate all anomalies	CTO	Admin access to critical systems	Quarterly at regular management meetings or as needed for high-threat activity

Vulnerability Assessments: Perform quarterly vulnerability scans	Review dependabot to see what vulnerabilities are introduced and address high severity vulnerabilities within a quarter	CTO	vulnerability software	Quarterly at regular management meetings or as needed for high-threat activity
Compliance: Ensure compliance to our ISMS 100%	Review risk register and CAPA, address any gaps in compliance	CTO	personal	Quarterly at regular management meetings

These objectives consider our information security requirements and the risks and opportunities we have identified.

The Leadership Team ensures that our Information Security Objectives are:

- consistent with our Information Security Policy
- measurable
- monitored
- communicated
- updated as appropriate

These objectives and, where appropriate, the results of the Leadership Team's reviews are communicated to all employees, customers, suppliers, contractors, and interested parties.

When a process does not meet its objective(s) or encounters an unexpected problem, our Control of Corrective and Preventive Action Reporting Procedure is employed to research and resolve the issue and, wherever possible, improve the process.

6.1.2 Planning actions to achieve our Information Security Objectives

When planning how to achieve our Information Security Objectives, we determine:

- what will be done
- what resources will be required

- who will be responsible
- when it will be completed
- how the results will be evaluated, including indicators for monitoring progress periodically, or whenever our Information Security Objectives are changed. Change management

This process is conducted at least annually for inclusion in the annual information security management meeting.

7 Support

7.1 Resources

7.1.1 General

The Leadership Team ensures that all necessary resources are available to:

- implement and maintain our ISMS
- continually improve its effectiveness

Resources and resource allocation are assessed and monitored during information security management reviews.

7.2 Competency, and Awareness, and Communication

We operate and maintain arrangements to ensure competency, awareness, and communication.

These arrangements ensure that:

- all personnel are competent to undertake their tasks
- all personnel are aware of the following:
  - our management system(s) and their related policies and objectives
  - their roles and responsibilities
  - their contribution to the effectiveness of our management system(s)
  - the benefits of improved personal performance
  - the importance of complying with our management systems, policies, and procedures

- the consequences of any departure from our management systems, policies and procedures
- emergency preparedness and response requirements
- any management system changes
- the results of the Leadership Team's annual review of the management system(s) compared to their objectives

- training needs are identified
- appropriate training plans are developed and implemented

As appropriate, awareness programs are provided for contractors, temporary workers, visitors, etc., in addition to our staff.

7.3 Documentation and records

7.3.1 General

Our ISMS documentation includes both documents and records.

The Leadership Team has determined the extent of documented information:

- required by the ISO 27001:2022 and ISO 9001:2015 International Standard
- necessary for the effectiveness of our ISMS

Based on the following criteria:

- the size of our business
- the scope, complexity, and interaction of our processes and products/services
- the need to demonstrate fulfilment of our compliance obligations
- the competence of our personnel

PatientPartner maintains documentation practices that ensure all quality and information-security records are accurate, reliable, and compliant with ISO 9001 and ISO 27001 requirements. All entries must follow ALCOA principles—**Attributable, Legible, Contemporaneous, Original, and Accurate**—to preserve the integrity, traceability, and trustworthiness of documented information. Records must be created by authorized personnel, clearly identify who performed the activity, be readable and permanent, be completed at the time work is performed, and reflect the true and original source of information without unauthorized alteration. Good Documentation Practices require that all

records are dated, version-controlled, securely stored, and protected from loss, unauthorized access, or modification. Corrections must not obscure original entries and must include the reason for change, the person making the correction, and the date. These practices ensure that documented information remains complete, consistent, and reliable to support operational control, regulatory compliance, audit readiness, and continual improvement across the QMS and ISMS.

7.3.2 Control of documents (Paper and Electronic)

We operate and maintain arrangements for controlling the documentation of our quality management system,

Once established, all documented procedures are implemented and maintained.

7.3.3 Control of records

7.3.4 PatientPartner maintains all quality management system documents and records in a controlled and retrievable manner for a minimum retention period of **five (5) years**, or longer when required by applicable laws, regulations, contractual obligations, or explicit customer requirements. Records are protected from loss, unauthorized access, alteration, or degradation throughout their lifecycle, and remain legible, readily identifiable, and traceable to their originating processes. At the end of the defined retention period, records are securely disposed of in accordance with documented procedures unless an extended retention period is mandated by regulatory authorities or requested by the customer.

7.3.5 Archival

PatientPartner maintains all management system documents and records in a controlled and retrievable manner for a minimum retention period of five (5) years, or longer when required by applicable laws, regulations, contractual obligations, or explicit customer requirements. Records are protected from loss, unauthorized access, alteration, or degradation throughout their lifecycle, and remain legible, readily identifiable, and traceable to their originating processes. At the end of the defined retention period, records are securely disposed of in accordance with documented procedures unless an extended retention period is mandated by regulatory authorities or requested by the customer.

7.4 Customer Communications

PatientPartner ensures clear, timely, and controlled communication with customers regarding matters that affect service quality, data protection, and information security. Authorized personnel provide customers with accurate information about incidents, service changes, data-handling practices, and any issues that may impact the confidentiality, integrity, or availability of their information. PatientPartner maintains defined channels for customer inquiries, feedback, and complaints, and all communications are recorded and reviewed to support customer satisfaction, regulatory compliance, and continual improvement of both the QMS and ISMS.

8 Operations

8.1 Operational planning and control

The Leadership Team ensures that the processes needed to meet our ISMS requirements, address risks and opportunities, and establish and achieve our Information Security Objectives are adequately planned and controlled.

- we retain, analyze, and evaluate records to the extent necessary to have confidence that the processes have been carried out as planned
- we control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects
- when a process does not meet its objective(s), or an unexpected problem is encountered with a process, our Control of Corrective and Preventive Action (CAPA) Procedure is employed to research and resolve the issue and, wherever possible, improve the process
- we review this management system's suitability, adequacy, and effectiveness per our ISMS Management Reviews Meeting.

  These reviews include assessing our ISMS's continuing alignment with our strategic direction, opportunities for improvement, and the need for changes

8.2 Information security risk assessment

The Leadership Team ensures that information security risk assessments are undertaken, recorded, and retained periodically and when significant changes are proposed or occur.

These risk assessments consider our agreed risk assessment criteria and criteria for performing information risk assessments.

The risk assessment process includes:

- Risk identification, analysis, evaluation, treatment, reviews by management, the Statement of Applicability, and
- .00.
- ,.determined an acceptable risk criterion.
- Risk Likelihood shall be categorized by management as: Very Unlikely (1), Unlikely (2), Possible (3), Likely (4)
- Risk Impact shall be categorized by management as: Insignificant (1), Minor (2), Moderate (3), Major (4), Catastrophic (5)
- Inherent risk shall be categorized by management as: Low, Moderate, High
  Residual risk shall be categorized by management as: Low, Moderate, High,

8.3 Information Security Risk Treatment

We manage and control our risks through treatment as noted in our risk register

9 Performance Evaluation

9.2 Monitoring, measurement, analysis and evaluation

To evaluate the performance of our ISMS, we determine:

- what needs to be monitored and measured
- the methods of monitoring, measurement, analysis, and evaluation needed to ensure valid results
- the criteria against which we evaluate our information security performance and various indicators

- when such monitoring and measurement should be undertaken
- when the results from monitoring and measurement are to be analyzed and evaluated

These activities are used to evaluate:

- the performance and effectiveness of our ISMS
- the effectiveness of actions taken to address risks and opportunities
- the effectiveness of planning
- the performance of external providers
- other improvements to the management system

9.3 Internal audit

We operate and maintain arrangements for internal auditing at planned intervals at a minimum annually.

Using these audits, we provide information to management and determine whether our ISMS:

- conforms to our requirements
- conforms to the requirements of the ISO 27001
- is effectively implemented and maintained
- is effective in achieving our management system's policies and objectives

9.4 Management Review

We operate and maintain annual arrangements for reviewing our ISMS's suitability, adequacy, and effectiveness. These reviews include assessing our ISMS's continuing alignment with our strategic direction, opportunities for improvement, and the need for changes, as outlined below.

The meetings will cover:

- The status of actions from previous management reviews.
- Changes in external and internal issues relevant to the ISMS.

- Information on the performance and effectiveness of the ISMS, including trends in nonconformities and corrective actions, monitoring and measurement results, audit results, and the fulfillment of information security objectives.
- Feedback from interested parties.
- Results of risk assessment and status of risk treatment plans.
- Opportunities for continual improvement.

The outcomes of the management review will include decisions and actions related to:

- Improvement of the ISMS and its processes.
- Resource needs.
- Any need for changes to the ISMS.

10 Improvement

10.2 General

We continuously use our ISMS and other inputs to improve our information security outcomes.

The improvement opportunities include:

- addressing evolving and future needs and expectations reviewed annually with our management review meeting
- correcting, preventing, and reducing undesired effects
- improving the performance and effectiveness of our ISMS

10.3 Non-conformity and corrective action

We operate and maintain arrangements to take corrective action to eliminate and further prevent the cause of any non-conformity and preventive action to eliminate the causes of potential similar non-conformities, as set out in our Control of Corrective and Preventative Action Reporting (CAPA) Procedure.

10.4 Continual improvement

We seek to continually improve our ISMS's suitability, adequacy, and effectiveness.

We use the results of analysis and evaluation and the outputs from information security management reviews to identify needs and opportunities for improvement.

Our information security management review process monitors and assesses the overall effectiveness of our continual improvement program, including corrective actions and our wider progress in achieving corporate-level improvement objectives. It is included in the agenda for the annual management review meeting.

10.5 Customer Complaint Management Procedure

PatientPartner maintains a structured and controlled process for receiving, recording, evaluating, and resolving customer complaints related to our patient-support services and SaaS platform. All complaints submitted by our customer or partner organizations are documented and reviewed to determine their impact on product quality, service performance, regulatory obligations, and customer satisfaction.

Upon receipt of a complaint, PatientPartner will record the details, assess the nature and severity of the issue, and determine whether corrective and preventive action (CAPA) is required. Complaints indicating systemic issues, repeated failures, potential patient safety concerns, or nonconformities affecting compliance will be escalated for formal CAPA evaluation. All actions taken, including decisions not to initiate CAPA, will be documented and retained as part of the Quality Management System.

Minimum Complaint Record Content

- Date received
- Name of complainant and organization (if applicable)
- Description of the issue
- Affected product, feature, or service
- Initial assessment and severity classification
- Decision on whether CAPA is required
- Actions taken and resolution
- Date of closure

PatientPartner reviews complaint trends as part of ongoing performance evaluation and uses this information to drive continual improvement of the QMS and the services provided to healthcare professionals and their patients.

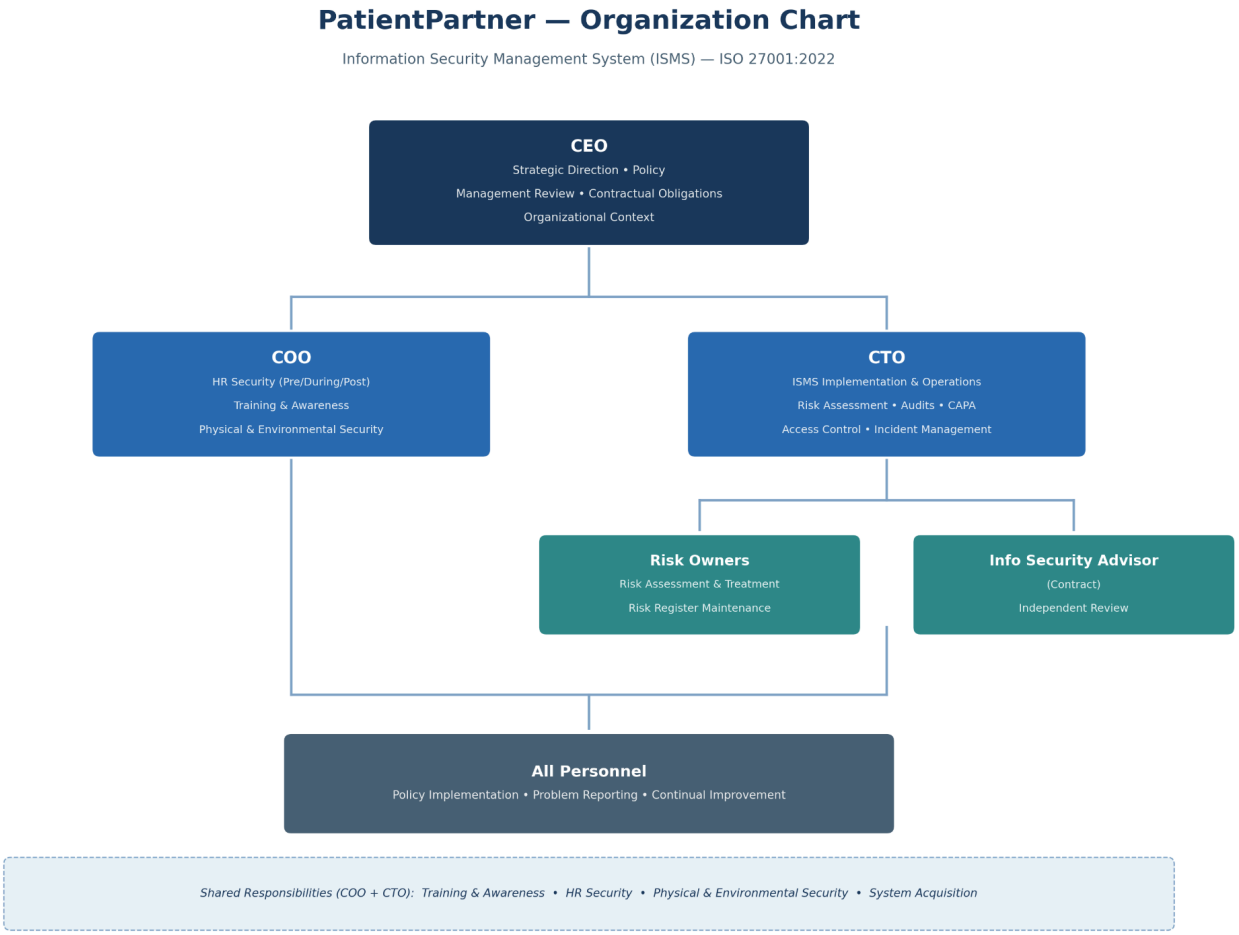
11 Annex A – Control Objectives and Controls

We adopt those information control objectives in Annex A of ISO 27001:2022 as appropriate based on the Patient Partners risk assessment and add additional control objectives and controls where necessary.

Revision history

Revision	Date	Record of Changes	Approved By
0	15AUG2024	Initial Issue	Zhichao Han
1	01OCT2025	Annual Review	Zhichao Han
2	01MAR2026	Quality Systems Requirement Updates	Zhichao Han

12 Appendix 1 - Organization Chart



13 Appendix 2 - Organisational High-Level Process Map

