November 2022

INFORMATION SECURITY POLICY

1. INTRODUCTION

PURPOSE

This is the Information Security policy of Prescient Healthcare Group. This policy supersedes all of the company's earlier policies relating to health and safety at work and is applicable to all employees of Prescient Healthcare Group companies.

The Board of Directors and management of Prescient Healthcare Group, located at CP House, 97-107 Uxbridge Rd, London, W5 5TL are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets, including personally identifiable information (PII), throughout the organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information, privacy and information security requirements will continue to be aligned with Prescient Healthcare Group's goals, and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information and privacy related risks to acceptable levels.

SCOPE

Prescient Healthcare Group is committed to ensuring compliance with all applicable legislative, regulatory and contractual requirements, including all applicable PII protection legislation. Prescient Healthcare Group's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information and privacy related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information and privacy related risks are controlled. The Head of Risk is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

Business continuity and contingency plans, data backup procedures, avoidance of viruses and criminal hackers, access control to systems, and information security and privacy incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Information Security Manual and are supported by specific documented policies and procedures.

Prescient Healthcare Group aims to achieve specific, defined information security and privacy objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

RESPONSIBILITIES

All Employees/Staff of Prescient Healthcare Group are expected to comply with this policy and with the ISMS that implements this policy. All Employees/Staff, and certain external parties, will receive appropriate training. The consequences of breaching the information security and privacy policies are set out in Prescient Healthcare Group's disciplinary policy and in contracts and agreements with third parties. The Chief Financial Officer is currently ultimately responsible for this policy with oversight responsibility from The Board of Directors and management of Prescient Healthcare Group.

COMPLIANCE MEASUREMENT

The ISMS is subject to continuous, systematic review and improvement. Prescient Healthcare Group is committed to achieving certification of its ISMS to ISO 27001:2013, and its continual improvement.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan at least annually.

2. INFORMATION SECURITY

In this policy, 'Information Security' is defined as:

2.1 Preserving

2.1.1 This means that management, all full or part-time Employees/Staff, sub-contractors, project consultants and any external parties have, and will be made aware of, responsibilities (which are defined in their job descriptions or contracts) to preserve information security and privacy, to report security and privacy breaches (in line with the policy and procedures identified in section 16 of the Information Security Manual) and to act in accordance with the requirements of the ISMS. All Employees/Staff will receive information security and privacy awareness training, and more specialised Employees/Staff will receive appropriately specialised information and privacy security training.

2.2 Confidentiality

2.2.1 This involves ensuring that information is only accessible to those authorised to access it and therefore preventing both deliberate and accidental unauthorised access to Prescient Healthcare Group's information and its systems.

2.3 Integrity

2.3.1 This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency and data backup plans along with security and privacy incident reporting. Prescient Healthcare Group must comply with all relevant data and privacy related legislation in those jurisdictions within which it operates.

2.4 Availability

2.4.1 This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and Prescient Healthcare Group must be able to respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

2.5 Physical Assets

2.5.1 The physical assets of Prescient Healthcare Group, including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

2.6 Information Assets

2.6.1 The information assets include information (whether PII or otherwise) printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e., the software: operating systems, applications, utilities, etc.).

2.7 Prescient Healthcare Group

2.7.1 Prescient Healthcare Group and the ISMS is the information security management system, of which this policy, the Information Security Manual and other supporting and related documentation are a part, and which has been designed in accordance with the specifications contained in ISO 27001:2013.

2.7.2 A **security breach** is any incident or activity that causes, or may cause, a breakdown in the confidentiality, integrity or availability of the physical or electronic information assets of Prescient Healthcare Group.

2.7.3 A **privacy breach** is any incident or activity that causes, or may cause, a breakdown in the confidentiality, integrity or availability of the PII assets of Prescient Healthcare Group.

3. GOVERNANCE

3.1 Document Owner and Approval

3.1.1 The Data Protection Officer is currently the owner of this document and is responsible for keeping it up to date.

3.1.2 The current version of this document is available and is published.

3.1.3 Approval status can be viewed in the Master List of Document Approval.

3.2 Policy Review

3.2.1 This policy shall be reviewed regularly by the Prescient Healthcare Group's Data Protection, Compliance, and Information Technology departments and should be amended to reflect any changes in law or practice. The Board should monitor this policy at least annually and through periodic review of Internal Audit findings by the Audit Committee.

3.3 Document History

Version	Date	Comment	Owner
0.1	2019-04	First draft	Ross Fenwick
0.2	2019-05	Second draft	Ross Fenwick
0.3	2019-06	Final draft and sign-off	Nick Denison-Pender
1.0	2019-06	Release	Ross Fenwick
1.1	2020-04	Aligned to ISO27001	Ross Fenwick
1.2	2021-04	Review	Nick Denison-Pender
1.3	2022-04	Review	Nick Denison-Pender
1.4	2022-11	Update to incorporate commitment to continual improvement and board responsibility based on feedback from ISO27001 Gap Analysis conducted in September 2022.	Ross Fenwick
1.5	2022-11	Review and sign-off	Alex Panayi