SENSYNE HEALTH

INFORMATION SECURITY AND INFORMATION GOVERNANCE

03 FEBRUARY 2020

Designed by Clinicians. Focused on patients. Powered by AI

Document Template Details and Quality Control

<table>
<tr><td>Document Name</td><td colspan="4">Sensyne Health – Information Security and Information Governance</td></tr>
<tr><td>Description</td><td colspan="4">This document provides a brief overview of the measure in place to control the security of the information generated by Sensyne Health or entrusted to Sensyne Health in the course of its activities. The guidance described here makes reference to several internal procedures that form integral part of our Quality Management System and that can be made available upon request.</td></tr>
<tr><td>Ref. No.</td><td colspan="4">CORP.BR.20.02.03</td></tr>
<tr><td>Current Version</td><td colspan="4">V2.0</td></tr>
<tr><td>Publication Date</td><td colspan="4">03 February 2020</td></tr>
<tr><td>Confidentiality</td><td colspan="4">Public Information</td></tr>
<tr><td rowspan="3">Document Version History</td><td>Date</td><td>Version</td><td>Name</td><td>Reason for Change</td></tr>
<tr><td>31/01/2020</td><td>1.0</td><td>Roberto Liddi</td><td>First version</td></tr>
<tr><td>03/02/2020</td><td>2.0</td><td>Kam Ahumibe/James Chandler</td><td>Feedback added</td></tr>
<tr><td>Contact details for further information</td><td colspan="4">Sensyne Health plc
Schrödinger Building,
Heatley Road, Oxford Science Park,
Oxford, OX4 4GE

+44 (0) 330 058 1845
info@sensynehealth.com</td></tr>
</table>

Table of Contents

1. Introduction

Sensyne Health plc is a British healthcare technology company that creates value from accelerating the discovery and development of new medicines and improving patient care through the analysis and commercialisation of real-world evidence from large databases of anonymised patient data in collaboration with our NHS Trust partners, to solve serious unmet medical needs across a wide range of therapeutic areas.

What we do:

- License the use of our proprietary digital health software products to healthcare providers, connecting patients, clinicians and researchers to improve patient care
- Build large databases of anonymised patient data in collaboration with NHS Trusts
- Analyse the datasets using proprietary clinical artificial intelligence algorithms
- Discover new insights that improve patient care within the NHS or which are of significant value to pharmaceutical companies in the development of new medicines and file patents to protect them
- License this IP to pharmaceutical companies in return for research fees, milestone payments and royalties
- Share the returns generated with NHS Trusts via equity and a royalty on Sensyne Health revenues

Sensyne Health has been set up to be an exemplar of how a commercial company can partner with the NHS to improve patient care and generate value from anonymised patient data in an ethical way.

Anonymised patient data is ethically sourced in that any analysis of anonymised patient data (and hence the Company's access to it) must be pre-approved for each programme on a case-by-case basis by the relevant NHS Trusts. This is to ensure that the purpose of the anonymisation and the proposed analysis are subject to appropriate ethical oversight and information governance, including conformance with NHS principles, UK data protection law and applicable regulatory guidance.

Sensyne Health's mission is to use its proprietary clinical artificial intelligence technology to analyse ethically sourced, clinically curated, anonymised patient data in partnership with leading NHS Trusts to solve serious unmet medical needs across a wide range of therapeutic areas.

The confidentiality, integrity and availability of information, in all its forms, are critical to the ongoing functioning and good governance of Sensyne Health. Responsibility for all information security and information governance issues are managed by the Information Governance Lead who reports directly to the Board.

2. Intended audience

The information contained in this document is available to those individuals or teams seeking clarification on how Sensyne Health operates under current Information Security and Governance requirements.

3. Summary of key terms

ISO27001 - ISMS	Information Security Management System
GDPR	General Data Protection Regulation
SIRO	Senior Information Risk Owner
CG	Caldicot Guardian
IG Group / Team	Information Governance Group / Team
IAO	Information Asset Owner
DPA	Data Protection Act 2018

4. Sensyne Information Security framework

Information Security compliance is ensured by means of external certification to ISO27001, which includes specific requirements dictated by GDPR and by internal procedures that address further defined requirements mandated by data protection legislation and security management system.

The internal procedures that address Information Security requirements are part of Sensyne Quality Management System as follows:

- GDPR (QP29) Policy was updated version 2
- SOP17 DPIA procedure – FM23 and FM24
- SOP20 Data Breach Reporting – FM31
- SOP21 Data Subject Access Request – FM32, FM33 and FM34
- SOP27 Security Incident Management

Sensyne Health is registered with the ICO (Information Commissioner's Office) as required by GDPR and DPA 2018 (registration number ZA451278).

Sensyne Health has been assessed against the DPS (Data Protection and Security) Toolkit (March 2019 version). Our assessment has been published as required by NHS Digital (DSP Toolkit number 8K382). The Data Security and Protection Toolkit is an assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

Sensyne Health is certified against ISO27001, Information Security Management System by BSI (British Standards Institution) with Certificate number IS 707857, with the following certification scope: "The protection of information and data assets for the delivery of Sensyne Health services and activities. The assets protected are physical locations, hardcopy and/or electronic data and IT hardware. Technology includes server platforms and organisational networks hosted on cloud services within the control of Sensyne Health, in accordance with Sensyne Health Statement of Applicability Ver 3 10/22/19"

BSI regularly audits Sensyne's premises in order to ensure continuous compliance.

ISO27001 is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes. It is worth noting that Annex A of the standard lists over 100 security controls which bring together physical security, operation and communication security, HR management, incident management, business continuity, organisational issues and legal compliance along with IT management controls specific for each organisation.

Further internal procedures allow exact identification, control and change management of each identified Sensyne asset, ensuring that at any given point in time full reporting and traceability are available.

Sensyne Health is also certified under the ISO13485, regulatory requirements for medical device manufacturers. Under such standard, Sensyne is required to constantly monitoring its performance and compliance by means of scheduled internal audits. At Sensyne, we have combined the requirements of both ISO27001 and ISO13485 standards in a single audit program which is deployed by a pool of externally certified auditors. Such plan gives assurance and reports to the Senior Management that proper control and management of Sensyne's activities are regularly monitored.

Sensyne Health also has strict internal security measures – information is held in an encrypted form in a secure internal server location accessed only in Sensyne Health's 'cold room', a physically secure environment with strict access control, CCTV recording and physically isolated (or 'air gapped) from any outside networks/open internet access.

No anonymised patient level data is ever shared with Sensyne Health's pharmaceutical partners. Only Sensyne Health data scientists, machine learning researchers and biostatisticians have access to data for analysis and only from the physical location where the data is held for the duration of the analysis. It is only the results of the analysis that are commercialised and therefore shared with pharmaceutical partners. Sensyne Health does not sell or share anonymised patent data with any third parties.

Physical access control to the 'cold room' facilities is strictly granted, controlled and regularly audited by Sensyne IG team.

5. Information Governance framework

Sensyne Information governance framework is based on GDPR principles and requirements related to information sharing and processing which are translated into internal procedures and forms that, just like in the case of Information Security, constitute an integral part of our Quality Management System:

- SOP22 Data Request and Processing
- QP07 Privacy Policy
- FM33 Data Processing Protocol Form
- FM36 Aggregate Information Request Form

Every NHS Trust or third party that enters into a data sharing project with Sensyne, is required to sign a SRA (Strategic Research Agreement) that defines the purpose, roles and responsibilities of each party. Such agreements refer heavily to the definitions given within the GDPR/DPA2018 with respect to Data Controller and Data Processor. Such Strategic Research Agreements allow Sensyne to receive **anonymised** patient data from the Trust partners for the purpose of scientific research. Although recital (26) of the GDPR clearly states that "*the principles of data protection should therefore not apply to anonymous information*", Sensyne has chosen to comply to all principles and requirement of current data protection legislation for the purpose of transparency. This means that a dedicated team within Sensyne, including a DPO (Data Protection Officer), a CG (Caldicott Guardian), a SIRO (Senior Information Risk Officer) and an IAO (Information Asset Owner), oversee all those activities that require data transfer, movement and/or control prior to the data being released for research analysis. In particular, the Data Request and Processing procedure, which is also agreed with the partner Trusts, explains in details the data flow and governance control steps and establishes that the partner Trust is always acting as Data Controller, therefore keeping control of the shared data even in an anonymised form.

6. Conclusion

The Information Security and Governance Frameworks that Sensyne has set up, exceeds regulatory and legal requirements to ensure an ethical, transparent and compliant approach to data sharing and processing activities under the current data protection legislation.