OPEN Health
Global Information Security Minimum Standards for Suppliers
v1.0

Issued by:	Governance and Compliance
Audience:	All Supplier Organisations
Purpose	Ensure we adhere to the minimum Information Security standards as required by law and our Clients
Published	October 2022

1.0 Introduction/Purpose

OPEN Health places the utmost importance on Information Security and has set the following objectives:

- safeguard and protect information, ensuring the preservation of the confidentiality, integrity, and availability of the data;
- establish safeguards to protect information resources from theft, abuse, misuse, or any form of damage;
- encourage the management and staff to maintain an appropriate level of awareness, knowledge, and skill to allow them to minimize the occurrence and severity of security incidents; and
- ensure that any company doing business with OPEN Health can continue its commercial activities in the event of significant Information Security incidents.

To help meet these objectives, OPEN Health requires that any suppliers with access to OPEN Health data, IT infrastructure, or systems have sufficient security controls in place. These include (but are not limited to):

- Have in place an accredited IT Managed Service Provider (MSP) or an MSSP (Managed Security Service Provider) to operate the core information technology systems or a team sufficiently resourced to operate and manage the information security function.
- Have a Network Operating Centre (NOC) and a Cyber Security Operation Centre (CSOC) for monitoring security aspects across any OPEN Health data or a process for monitoring, reviewing, and auditing security controls.
- Have engaged a Security Ratings Company to scan and report on web anomalies every 24 hours for all web components that reside outside the networked environment or have regular audits of its internal and external infrastructure.

In addition, OPEN Health requires the following technological and organisational measures to be implemented:

2.0 Physical Admin Control & Security

1. Offices are protected by alarm systems and require RFID passes in order to gain access.
2. Surveillance exists at data centres where OPEN Health data will be stored.
3. Processes are in place for the management and recording of visitor access to offices, data centres, or other areas containing sensitive information.

3.0 Virtual Admin Control

1. Unique passwords are assigned to every individual and exclusions are applied for excessive attempts.
2. Access to data is managed strictly via 'least privilege' protocols to ensure that only the required staff have access to the data.
3. Anyone working remotely must sign in via a Virtual Private Network (VPN) with two-factor authentication to access any OPEN Health data.
4. Everyone must sign in via two-factor authentication to access any cloud-related service.

4.0 Network Protection

1. Antivirus software must be in place and will be constantly active, on all end-point devices, servers, and cloud entities.
2. All physical network equipment is hardened and default passwords changed as part of any implementation process.
3. Appropriate patching schedule(s) are in place to apply security updates to all end-point devices and server operating systems consistently and regularly.
4. Patches are applied in appropriate timescales subject to manufacturers' recommendations.
5. Penetration and vulnerability tests are performed regularly, especially related to data held/processed for OPEN Health.

5.0 Encryption

1. Laptops, mobile devices (such as mobile phones, tablets, smart watches, USB, and other portable storage devices), file servers, and internal Wi-Fi are encrypted.
2. Storage used as part of any cloud service is encrypted.

6.0 Data Availability

1. There is close to real-time replication of any OPEN Health data from primary to secondary data centre(s), if applicable.
2. Separate and independent backups are performed in both (if applicable) primary and secondary data centres.

7.0 Data Privacy

1. OPEN Health must be informed of any data privacy breach within 24-hours.
2. Processes in place to adhere to Global Data Privacy Regulations, including Data Subject Rights Requests, within the legal limits.
3. Data processing agreements are required for third parties accessing OPEN Health data.
4. Safeguards are in place for any international transfers not covered by an adequacy decision.
5. Processes are in place to protect data privacy in the event of an acquisition or merger, new system implementation, systems development, or equipment changes.

8.0 Organisational Measures

1. IT/Information Security Policy is in place.
2. Security and data incidents shall be managed by following an incident management process and response plan.
3. Full cooperation with OPEN Health is required with regard to any security investigation regarding potential breaches of your information security obligations.
4. Any/all system changes (including user/desktop [for adds, moves, and deletions], server, and network changes) are managed via strict change control processes.
5. Use of nondisclosure agreements and confidentiality agreements to secure OPEN Health data with staff and third parties is required.
6. IT Security assessments are required for any third-party accessing IT infrastructure or OPEN Health data.

End of Document