

Health Shield Information Security Summary Statement of Services

Table of Contents

Introduction 3

Information Security and Continuity Governance 3

Supplier Management 3

Access Management 3

- Customer Access Management 3
- Health Shield Employee Access Management 3
- Privileged Access Management 4

Intrusion Detection and Monitoring 4

Data Encryption 4

Data Backup & Recovery 4

Protection of Service 5

- DDoS Protection 5
- High-Availability and Resilience 5
- Network and Operations Security 5
- Physical Security 5
- Vulnerability and Patch Management 6

Data Protection 6

- Data Protection Officer 6
- Policy and Procedural Documentation 6
- Employee Training and Awareness 6
- Privacy Notices 6
- Record of Processing Activity (ROPA) 6
- Data Processing Agreements 7
- Data Protection Impact Assessments (DPIAs) 7
- International Data Transfers 7

Introduction

At Health Shield, the security and protection of client data is our top priority. This statement is provided as a summary of Health Shield practices relating to information security.

Information Security and Continuity Governance

Health Shield Friendly Society has mature Information Security Management (ISMS) and Business Continuity Management Systems (BCMS), which are certified to the ISO27001:2022 and ISO22301:2019 standards respectively. Both systems are audited annually by an ASCB accredited external auditor.

Health Shield's customer facing portals are built on the Microsoft Azure platform. Microsoft is certified to multiple global, regional, and industry-specific security standards, which are available to review here: https://servicetrust.microsoft.com/.

Health Shield's IT systems are built on Microsoft platforms and co-located in a resilient UK data centre. Our data centre is certified to multiple global standards, which are available to review here: https://www.equinix.com/data-centers/europe-colocation/united-kingdom-colocation/manchester-data-centers/.

Supplier Management

Health Shield ensures strong supplier management governance with formal procurement and supplier management frameworks in place to support optimum, auditable supplier engagements and management. Through our frameworks, Health Shield conducts financial, privacy and security due diligence checks, maintain contracts and confidentiality agreements with all suppliers and many other supplier health activities. Enhanced checks are applied to suppliers who access, store, or process data, supported by our Data Protection Officer (DPO) and the application of UK GDPR and other applicable data protection legislation.

Access Management

Identity and Access Management (IAM) and Customer Identity Access Management (CIAM) solutions ensure that the data that Health Shield holds is secured.

- **Customer Access Management**

Multi-factor authentication options on Health Shield's portal environments is offered to all Members and Customers of Health Shield services.

- **Health Shield Employee Access Management**

Health Shield has formal user access provisioning procedures for employee access to environments or systems that access, store or process customer data, controlled by role-based access permission sets that are reviewed regularly to ensure compliance with needs is maintained.

The Least Privilege principle is used for access to environments or systems that access, store or process data.

Multi-factor authentication is enforced for all remote employee access to environments or systems that access, store or process data.

Health Shield enforce password changes at a maximum of every 90 days and implement strict password complexity rules.

- **Privileged Access Management**

Privileged users are provided with an account separate to their standard account and provided with the absolute minimum access rights required to fulfil their business role. Privileged account creation and change must be approved by an appropriate authority.

Each privileged account must be uniquely identifiable, monitored by Security Information and Event Management (SIEM), and subject to strong multi–factor authentication.

Privileged access to networks, computer systems, applications and facilities is regularly reviewed and is subject to the Starters, Movers, Leavers section of the Access Control Policy.

Intrusion Detection and Monitoring

Device logs from systems across the Health Shield IT estate are ingested into a centralised SIEM platform. This includes the following, but is not limited to, servers, next-gen firewalls, networking devices, XDR platform, cloud platforms, authentication, and email services. The SIEM platform is monitored 24/7 by a specialist Security Operations Centre (SOC).

A centrally managed Extended Detection and Remediation (XDR) software is used on all devices that access data. XDR alerts are monitored 24/7 by a specialist Security Operations Centre (SOC).

Data Encryption

All data in transit is encrypted using Transport Layer Security (TLS) 1.2 or 1.3.

All data backups are encrypted at rest using industry-standard, FIPS-certified 256-bit Advanced Encryption Standard (AES-256).

Data Backup & Recovery

Backup data is crucial for protecting against data loss due to accidental deletion, corruption, system failures, or malicious intent.

All critical data, including records, attachments, documents, and metadata, are included in scheduled backups to ensure comprehensive data protection and the ability to recover rapidly from an incident.

Backups are immutable and stored securely online in cloud platforms with access to data stores strictly limited to resources located within the EU.

Protection of Service

Health Shield's IT systems utilise high availability technologies, supported by the benefits of data centre hosting. There are multiple layers of protection in place to ensure that service continuity is maintained including N+1 cooling and power.

Microsoft Azure secures its global data centres using a multi-layered defence model. This combines strict physical perimeters, hardware-rooted trust, and default encryption with highly resilient regional architecture, and availability zones.

- ### DDoS Protection

A Web Application Firewall (WAF) is used to provide protection to all platforms against Distributed Denial-of-Service attack.

Additionally, Microsoft Azure offers DDoS Shielding to automatically defend infrastructure against Distributed Denial-of-Service attacks.

- ### High-Availability and Resilience

All elements of the Health Shield IT environment are designed with resilience in mind, including redundant power, data, firewall, server and cooling.

Microsoft Azure utilises Availability Zones - separate physical data centres within a region feature independent power, cooling, and networking; and Paired Regions - Geographically separated regions to ensure geo-redundant backups and seamless failover.

- ### Network and Operations Security

A centrally managed Endpoint Detection and Remediation (EDR) software platform is used on all devices that access data. EDR alerts are monitored and remediated 24/7 by a specialist Security Operations Centre (SOC).

Mobile Device Management software is enforced on all company owned devices and the use of personal devices for accessing, storing or processing customer data is prohibited.

Formal Change Management procedures are followed for all changes to systems and environments that access, store or process customer data.

- ### Physical Security

Health Shield IT data centre environment is provided by Equinix who, in common with Microsoft Azure, take a layered approach to physical security:

  - **Perimeter layer:** covering physical access permissions to the data centre site, monitoring for unauthorised entry to property, video surveillance, intrusion detection, and access log monitoring.
  - **Infrastructure layer:** covering physical access to infrastructure, diagnostics on machines, networks, and backup equipment.

- **Data layer:** covering access to data, threat and electronic intrusion detection systems, fortified access points to server rooms, monitoring and maintenance of media storage devices.
- **Environmental layer:** covering redundant power, networking and cooling.

- **Vulnerability and Patch Management**

Health Shield maintains a formal Vulnerability and Patch Management programme designed to identify, assess, and remediate security vulnerabilities in a timely manner. The effectiveness of our security controls is independently assessed through annual penetration testing, with identified vulnerabilities tracked and remediated based on risk.

Operating systems and applications are routinely patched on a monthly basis, with ad hoc patching performed where critical or actively exploited vulnerabilities require urgent remediation.

Health Shield also utilises relevant threat intelligence reports to maintain awareness of emerging threats and vulnerabilities and to inform prioritisation and remediation activities.

Data Protection

- **Data Protection Officer**

Health Shield have appointed a Data Protection Officer who ensures compliance with data protection laws, advises on privacy risks, monitors and audits data handling practices, and serves as a point of contact for data subjects and regulators.

- **Policy and Procedural Documentation**

Health Shield have reviewed and updated all policy and procedural documentation to align ourselves with relevant data protection laws and standards. Our framework of policies have been reviewed, amended, approved, published and communicated to employees throughout the organisation. Policies are reviewed and approved every 12 months.

- **Employee Training and Awareness**

We ensure that every member of staff at Health Shield has completed data protection training and awareness sessions, tailored to their job role, with our Data Protection Officer.

- **Privacy Notices**

We review and maintain all privacy notices to meet the compliance standards set out in the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR). Our privacy notice is available on our website.

- **Record of Processing Activity (ROPA)**

In line with our record keeping obligations set out in the Data Protection Act 2018 and UK GDPR, as both a Data Controller and Data Processor, we have documented our processing activities. This includes where Health Shield act as a both a Controller and a Processor.

- **Data Processing Agreements**

Where Health Shield act as a Controller, we have ensured that we only appoint Processors who can provide 'sufficient guarantees' that the requirements of the Data Protection Act 2018 and UK GDPR will be met and the rights of data subjects protected.

Agreements between Controllers and Processors ensure that parties understand their obligations, responsibilities and liabilities. Agreements help each to comply with the Data Protection Act 2018 and UK GDPR, and help Controllers to demonstrate their compliance.

Where we act as a Data Processor, our Terms & Conditions embed these requirements.

- **Data Protection Impact Assessments (DPIAs)**

Health Shield actively carries out Data Protection Impact Assessments (DPIA's) in line with Data Protection by Design and Default requirements in order for us to identify and minimise the data protection risks of a project or processing activity.

We ensure that DPIA's are performed where processing is likely to result in high risk to individuals.

- **International Data Transfers**

All data is processed in the UK and EU.

Statement reviewed September 2026