Radar Healthcare Compliance White Paper

QF33

radar
healthcare

Contents

Compliance White Paper

Introduction

At Radar Healthcare, we recognise how critical information security is in today's digital landscape. As an organisation entrusted with sensitive data, we're committed to maintaining the highest level of confidentiality, integrity, and availability of information assets. This Information Security Policy serves as a comprehensive guide to our information security practices, outlining our commitment to protecting data and mitigating potential risks.

Certifications and Standards:

ISO 27001 Certification:

We're pleased to share that Radar Healthcare has successfully achieved our ISO 27001 certification. This internationally recognised certification highlights our dedication to implementing a robust Information Security Management System (ISMS) and adhering to industry best practices. This demonstrates our commitment to safeguarding our systems and data against threats and vulnerabilities.

DSPT Standards Exceeded:

Radar Healthcare exceeded the requirements set forth by the Data Security and Protection Toolkit (DSPT). Our proactive approach to information security ensures that we go above and beyond the minimum standards, continually enhancing our security controls and risk management processes. By surpassing these standards, we demonstrate our commitment to the protection of personal and sensitive information.

Cyber Essentials Certification:

Radar Healthcare has also obtained the Cyber Essentials Certification. This certification validates that we have implemented essential security measures to defend against common cyber threats. Attaining this certification reinforces our proactive stance towards cybersecurity and our dedication to securing our systems and data.

Data Protection:

At Radar Healthcare, we take our commitment data protection very seriously. We recognise that data is a valuable asset and a fundamental component of our business operations. We are committed to ensuring the confidentiality, integrity, and availability of data under our care.

We implement a range of technical, administrative, and physical controls to secure our systems and data. These measures include but are not limited to strict access controls, encryption of sensitive information, regular vulnerability assessments, and robust incident response procedures. Our personnel are regularly trained on data handling best practices to ensure compliance with relevant privacy regulations and industry standards.

Furthermore, we maintain a culture of data security awareness throughout the organisation. All employees are responsible for adhering to our information security policies, reporting any potential security incidents promptly, and actively participating in ongoing security training and awareness initiatives.

FAQs:

Subject: Information Security

Question 1:

Can you confirm that Radar Healthcare complies with industry standards of information security good practice ISO/IEC 27001 or equivalent?

Answer:

Radar Healthcare confirms that it is fully compliant with information security standards. It holds ISO27001 certification from NQA (certificate number 187850). Additionally, Radar Healthcare has obtained the Cyber Essentials certification, Cyber Essentials Plus, and is HIPAA compliant.

Question 2:

Please provide details of your policies and procedures to ensure compliance with international data privacy laws.

Answer:

Radar Healthcare operates internal policies, including our QF06 Data Protection Policy, to ensure correct management of all data and compliance with legal obligations. The company fully embraces the requirements of GDPR and has invested in the necessary resources, processes, and structures to ensure GDPR compliance. Incident response processes are in place to promptly report any breaches. Hosting providers also employ various processes and standards, including annual penetration testing, to prevent data breaches.

Question 3:

How does Radar Healthcare ensure that they are compliant with the General Data Protection Regulation (GDPR) regarding breaches?

Answer:

Radar Healthcare has fully embraced the requirements of GDPR and has dedicated resources, processes, and structures to ensure compliance. In the event of a breach, an incident response process is established, allowing for efficient communication to both the affected party and the ICO (Information Commissioner's Office) within 48 hours of becoming aware of the incident.

Question 4:

Does Radar Healthcare notify of any 3rd party requests for data or information, including those of legal or administrative proceedings?

Answer:

Radar Healthcare does not pass any data onto third parties or partners by default. Data ownership lies with the customer, and Radar Healthcare would require permission before taking any action.

Question 5:

What are Radar Healthcare's policies on customers' rights for request to audit and audit rights?

Answer:

Details regarding customers' rights for request to audit and audit rights are included in the Radar Healthcare Service Level Agreement (SLA) and can be provided upon request.

Subject: Data Protection and System Security

Question 1:

What interfaces and systems are included in the contract?

Answer:

The contract includes the SiSense Analytics tool for providing dashboards, charts, and drill-down reports within the optional Analytics Builder License. Non-PID (Personally Identifiable Data) data is ingested into Radar Healthcare on an Azure install of SiSense.

Question 2:

Is all data encrypted across the network using TLS 1.2?

Answer:

Yes, all data is encrypted across the network using TLS 1.2.

Question 3:

How does Radar Healthcare ensure that data remains isolated from other customer data?

Answer:

Radar Healthcare ensures data isolation by design, with customers' data stored on separate database instances. This approach ensures that customer data remains isolated.

Question 4:

Please confirm how/if the data is encrypted at rest.

Answer:

All data is encrypted at rest through logical segregation in a vCloud Virtual Datacentre (VDC) on IaaS (Infrastructure as a Service). The encryption employs AES-256 XTS, making the data inaccessible if the disc is removed from the host without the TPM 2.0 module.

Question 5:

Can you confirm that all connections to remote servers and applications are authenticated?

Answer:

Yes, all connections to remote servers and applications require authentication. Only approved users, VPN (Virtual Private Network), and random number tokens are allowed access.

Question 6:

Can you confirm that access to diagnostic ports for network and server components is securely controlled?

Answer:

All ports are managed and secured in a Firewall as a Service by Redcentric. Access to diagnostic ports is limited to what is required for the application, ensuring secure control.

Question 7:

How do users authenticate into the system?

Answer:

Radar Healthcare provides standard Single Sign-On (SSO) via Security Markup Language (SAML). Best practice password management techniques are utilised, including automatic password expiry and the ability to enforce password changes.

Question 8:

What roles and different access levels are available for customers?

Answer:

Radar Healthcare operates with a comprehensive role-based approach, allowing system administrators to control permissions and access rights. During the implementation phase, business rules, roles, and associated permissions are pre-configured and can be applied on an individual or group basis.

Question 9:

Who Is the Data Protection Officer at Radar Healthcare?

Answer:

Radar Healthcare has a Data Protection and Quality Lead, Jonathan Alsop. The best way to contact Jonathan Is through our compliance email address: compliance@radarhealthcare.com

Subject: Data Backup and Audit

Question 1:

How often is data backed up?

Answer:

Radar Healthcare follows an industry-standard backup strategy. Servers are fully imaged every 24 hours for disaster recovery purposes. Transaction log backups of databases occur every 15 minutes to minimise the possibility of data loss. Full database backups are performed every 24 hours, with retention policies for daily, weekly, and monthly backups.

Question 2:

Does Radar Healthcare have an audit trail enabled?

Answer:

Yes, the Radar Healthcare system includes an Audit Log that automatically tracks every action undertaken by users. This log can be used for incident investigations or identifying user training needs.

Subject: Standards and Compliance

Question 1:

Does Radar Healthcare use the Data Security and Protection Toolkit (DSPT)?

Answer:

Yes, Radar Healthcare exceeds the requirements set forth by the Data Security and Protection Toolkit (DSPT) and continually enhances its security controls and risk management processes.

Question 2:

Are NHS Numbers available at the point of care?

Answer:

Where integrations allow, the Radar Healthcare system provides access to NHS Numbers at the point of care, enabling searching by the NHS number.

Question 3:

Is there a possibility of FHIR-based specifications?

Answer:

Radar Healthcare complies with FHIR-based specifications where required. An example in use is the Patient Demographics Query (FHIR API) with EPIV via App Orchard.

Question 4:

What identity services can be adopted?

Answer:

Radar Healthcare's authentication options can be extended to utilise FIDO and OpenID if required. Implementation and testing of these extensions would take approximately 3-6 months.

Question 5:

In terms of product design, do you comply with any other standards and practices?

Answer:

When designing the product, Radar Healthcare ensures compliance with standards set out by HM Government's Technology Code of Practice, NHS Digital, Data and Technology Standards, and the Government's Open Standards Principles. Compliance with relevant components of the NHSX Standards Framework and completion of the Digital Assessment Questionnaire (DAQ) are committed to where applicable.

Question 6:

What Is the size of Radar Healthcare's Security Team?

Answer:

Radar Healthcare's Security Team comprises of 4 members:

- Lee Williams, Chief Operating Officer
- Mike Taylor, Chief Technology Officer
- Jonathan Alsop, Data Protection and Quality Lead
- Scarlett Miller, Information Security and Quality Officer