connected healthcare :

responsive and resilient

Information Security and Data Protection Overview

For External Stakeholders

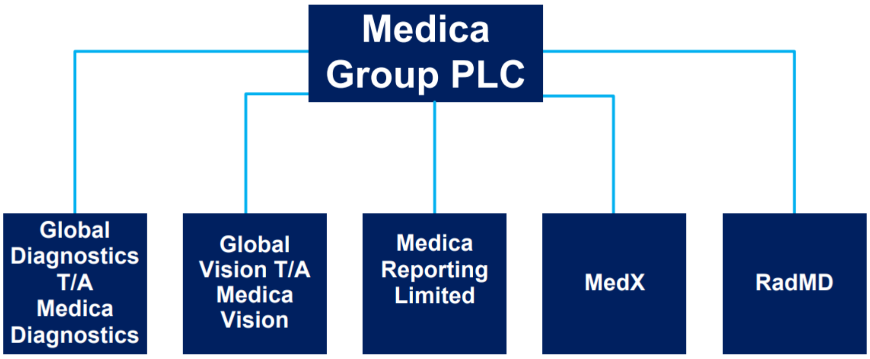
April 2022

Contents

Corporate Strategy and Structure 3
Governance & Risk Management 3
Accreditations and Certifications 3
Data Protection 5
What data are we responsible for as a Controller? 5
What data do we process whilst acting as a Processor? 5
Information Security 6
Incident Response 6
Business Continuity 7
Sub-contractor and Supplier Compliance 7
Stakeholder engagement 8
Data Lifecycle 8
Policies and Procedures 8

Corporate Strategy and Structure

Medica is committed to the security and protection of all data and information managed and processed through its group entities.

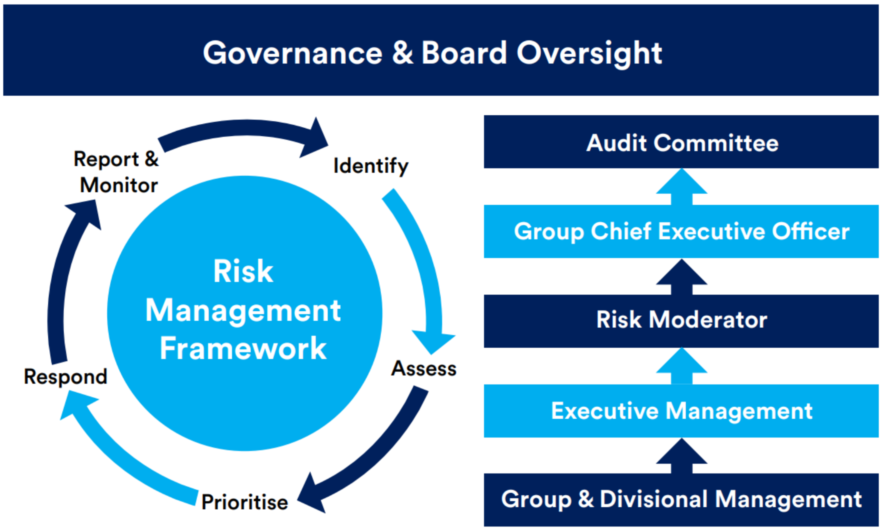

Medica Group PLC
Global Diagnostics T/A Medica Diagnostics
Global Vision T/A Medica Vision
Medica Reporting Limited
MedX
RadMD

This includes the assignment of a Group Chief Information Officer and the implementation of 'Data Owners', 'Data Stewards' and 'Data Custodians' based at individual entity level. Medica understands the duty of care required when processing data and what information security risks are most pertinent to our businesses. This document outlines the technical, operational, and physical controls in place to assure our external stakeholders.

Governance & Risk Management

Medica takes a risk-based approach to the governance of data and information. Details of our risk management framework and process can be found in the 'Risks and Uncertainties' section of our latest annual report. Risk registers are maintained across the Group, each is owned and reviewed on a regular basis, including Data Protection and Information Security.

Each risk is assessed using Medica's own risk scoring matrix to moderate and appropriately prioritise risks to the Group. The highest scoring risks are regularly reported on for ongoing monitoring and review by the Group's Audit Committee.


Governance & Board Oversight
Risk Management Framework
Identify
Assess
Prioritise
Respond
Report & Monitor
Audit Committee
Group Chief Executive Officer
Risk Moderator
Executive Management
Group & Divisional Management

Accreditations and Certifications

Medica is focused on maintaining the highest standards of quality and this mindset is applied to security and data protection. Medica has been certified and accredited to key standards and frameworks to enforce our practices. This is paramount to the Group's data protection and information security strategy

QSI QUALITY STANDARD FOR IMAGING UKAS MEDICAL 8311	Medica Reporting Limited has achieved accreditation with UKAS for the Quality Standard for Imaging.
CERTIFIED LR ISO/IEC 27001 UKAS MANAGEMENT SYSTEMS 001	Medica Reporting Limited holds a current ISO 27001 certification, the information security standard recognised globally.
CERTIFIED LR ISO 9001 UKAS MANAGEMENT SYSTEMS 001	Medica Reporting Limited and Global Diagnostics (T/A Medica Diagnostics) holds a current ISO 9001 certification, the international standard for quality management.
CHKS	Global Diagnostics (T/A Medica Diagnostics) holds a current CHKS accreditation, a European recognised standard in healthcare quality.
CYBER ESSENTIALS CERTIFIED	Medical Reporting Limited holds a current certification in Cyber Essentials, the national standard for cyber security in the UK as required by the NHS.
NHS Digital	Medica Reporting Limited is required to complete the NHS Data Protection and Security toolkit and meets the National Data Guardian's 10 Security Standards, a critical requirement to process patient data on behalf of the NHS.

Data Protection

Medica is committed to its obligations under data protection laws in particular in the UK and EU. We continue to monitor and taken necessary action to ensure that we meet our obligations as both a Data Controller and a Data Processor. Although Medica recognises that no organisation or business can be 100% compliant at all times, we do aim to operate within the compliance requirements of applicable privacy laws and regulations.

What data are we responsible for as a Controller?

- Employee data
- Sub-contractor data
- Client contacts and contractual data
- Supplier data

The legal basis for processing this data is a mix of contractual and legitimate interests. If legitimate interests are relied on for processing, then legitimate interest assessments (LIA) are carried out and approved.

What data do we process whilst acting as a Processor?

- Patient data (healthcare) – on behalf of all of our customers

The legal basis for processing special category healthcare data is overseen by each of our clients. We work with each client to support with the completion of data protection impact assessments (DPIAs) and to ensure that contractual compliance with privacy laws is appropriately maintained.

Medica has assigned a named Data Protection Officer, with overall responsibility for ensuring that Medica's privacy programme follows the UK and EU data protection regulations. This includes ensuring the following controls and activities are completed to comply with Medica's obligations as a Controller and Processor:

- Maintaining records of processing activity (ROPA)
- Publishing Privacy Notices – for staff, contractors, clients and patients (where required in co-ordination with our clients)
- Completion of Data Privacy Impact Assessments (DPIA)
- Completion of Legitimate Interest Assessments
- Registration with supervisory authority in relevant jurisdictions
- Review of data protection agreements and other contractual agreements

Information Security

Medica has a risk based information security management system that is used to monitor ongoing compliance with national and international information security standards and our own controls. The Group Chief Executive Officer has approved the following key objectives and each underpins Medica's approach to Information Security:

- Starters and leavers process whereby all starters leavers and movers are subject to a set change and approval process which is signed off by managers
- Scheduled penetration testing by our external CREST certified partner
- Quarterly external vulnerability scanning to ensure that our network is monitored for vulnerabilities
- Staff have access to and are required to read Medica's information security policies and procedures
- Employee vetting and checks, where all staff are subject to appropriate vetting, including criminal record checks where required
- We do not process card payments (PCI is n/a to our Group)
- Antivirus, antimalware and web filtering applied across the estate
- USB ports disabled by default

- Workstations with disk encryption
- Network accessible via encrypted VPN
- Use of our information classification system (Public, Restricted, Confidential)
- Privileged access controls for our administrator and privileged access accounts
- Secure physical perimeters, access control systems in place (key card entry)
- Programme of internal and external audits
- Secure development processes – against OWASP top 10
- Robust supplier management and continual review
- Regular monitoring and review of legal requirements

Incident Response

Breach and incident reporting requirements are documented in agreements with clients and in line with the requirements of the local supervisory authorities and regulators. Medica has dedicated personnel who are on hand to deal with information breaches or incidents that impact data and information security. The primary objective for incident response is mitigation and reducing potential impact. Investigations are carried out, with root cause analysis and actions documented for continual improvement of security practices.

Business Continuity

Business continuity is key to patient centric services. Medica implements continuity planning, processes and testing across the group to ensure that patient safety and turnaround times are prioritised.

Sub-contractor and Supplier Compliance

Medica's subcontractors and suppliers are subject to a process of vetting and validation of compliance with Medica's information security management system and data protection requirements. Our reporters are subject to vetting via recruitment and clinical governance for clinical competency and eligibility to work. Medica's process for supplier assurance will:

- Establish if they process personal data and the data types
- Establish the purpose of processing and legal basis for processing
- Establish if the supplier is a processor or sub-processor

If the supplier processes data we then explore the following questions:

- Process information for purchasing, invoicing and delivery?
- Have remote or direct access to Medica financial and/or business information?
- Have remote or direct access to Medica employee, reporter, or client patient information?
- Have access to existing Medica infrastructure or systems?
- Provide a critical service or product to Medica?
- How will quality service outputs be measured? (only applicable to Tier 1)
- Is the supplier financially stable?
- Pose an ICT Supply Chain risk?
- Pose a risk to Medica 's Information Security or product/service if the organisation fails or their service degrades?
- Have any security or other relevant industry certification(s)?
- Have appropriate privacy policies & data protection compliance in place?
- Use a website or cloud service to provide it's service(s) to Medica? If yes, include the web address used to access the service.
- Process any data outside of the UK or EU?

The supplier assurance is then completed by the security team who may give recommendations for further controls, such as non-disclosure agreements, data processing agreements and other contractual controls). The supplier is then approved or rejected by a member of the executive management team.

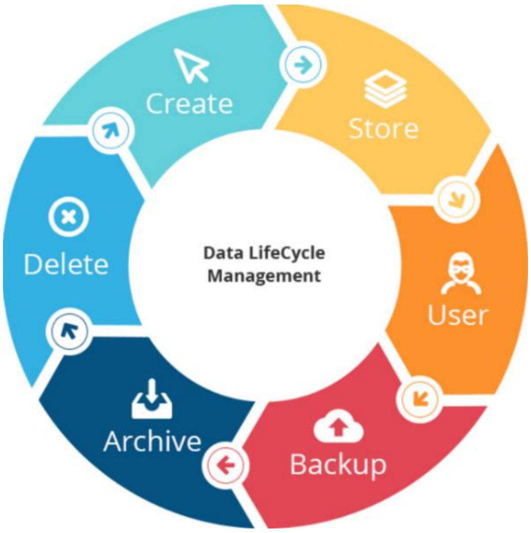
Stakeholder engagement

Medica engages with internal subject matter experts and external stakeholders for validation of compliance with requirements for information security and data protection. This can include the completion of Data Protection Impact Assessments, the sharing of penetration test results, logging of retention requirements or completing other information security and data protection assessments.

Data Lifecycle

All Data at Medica is subject to a defined lifecycle, and retention period. The lifecycle can defined for the purpose of:

- Meeting a contractual requirement
- Meeting a regulatory or legal requirement
- Meeting the requirement of the data subject
- Meeting a business requirement
- To ensure best practice



Policies and Procedures

In support of Medica's information security and data protection strategy, we have implemented the following policies which are available to all staff and contractors, and are reviewed at least annually or when there is a significant change:

- Data Protection Policy
- Information Security Policy
- Acceptable Use Policy
- Business Continuity Policy
- Access Control Policy
- Risk Management Policy
- Retention Policy
- Document Control Policy
- Network Security Policy
- Password Policy
- Clear Desk and Screen Policy
- Information Classification Policy
- Information Security Breach Management Policy

- Homeworking Policy
- Physical Security Policy
- Supplier Management Policy
- Safe Data Transfer Policy
- External information Sharing Policy
- Hardware and Software Control Policy
- Change Management Policy
- Employee code of Conduct