QMS LTD STATEMENT OF COMPLIANCE GDPR

INTRODUCTION

The EU General Data Protection Regulation ("GDPR") came into force across the European Union on 25th May 2018 and brought with it the most significant changes to data protection law in two decades. The Data Protection Act 2018 enshrines GDPR in UK law regardless of membership of EU.

QMS COMMITMENT

QMS are committed to ensuring the security and protection of the personal information that we process, and to providing a compliant and consistent approach to data protection. We have a robust and effective data protection program in place which complies with existing law and abides by the data protection principles, and Caldicott guidelines. This has been updated and expanded to meet the demands of the GDPR and the Data Protection Act 2018.

Our approaches to GDPR compliance are summarised in this statement.

HOW QMS COMPLIES WITH GDPR

QMS comply with GDPR in the following ways:

INFORMATION AUDIT

QMS carry out a regular company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and the legal basis for this processing. This includes both personal data we hold directly (as Data Controller), and data we hold and process on behalf of clients through contractual arrangements (as Data Processor).

POLICIES & PROCEDURES

QMS maintain data protection policies, procedures and documentation to meet the requirements and standards of the GDPR and any relevant data protection laws. This includes:

DATA PROCESSING ACTIVITY LOG.

QMS maintain a log of all processing of personal data, clarifying the data held, legal basis for processing, security arrangements, and subject access rights.

DATA PROTECTION IMPACT ASSESSMENTS (DPIA).

For all our client services, QMS acts purely as a Data Processor and QMS only processes data as defined in the Contract. Nevertheless, QMS undertakes DPIAs of all our services in conjunction with clients. We follow guidance from the Information Commissioners Office (ICO) using documentation processes that record assessments, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the client and to data subjects.

PRIVACY NOTICES

Where QMS holds personal data as the Data Controller, we produce a Privacy Notice to enable Data Subjects to understand how we process their personal data, and how their rights are protected.

Where QMS holds personal data on behalf of clients – as a Data Processor - QMS supports our clients to develop and maintain Privacy Notices for each service including describing the security and safeguarding arrangements during data transfer, data processing and storage, and subject access rights.

THIRD PARTY AGREEMENTS

Where QMS use third-parties or subcontractors to process personal information on our behalf, we have compliant Processor Agreements and due diligence procedures to ensure that they understand and meet GDPR obligations. These measures include initial and ongoing reviews of the service provided, and the third-party provision of GDPR compliant documentation. QMS review the necessity of the processing activity, and the third parties technical and organisational measures in place to ensure compliance with the GDPR. QMS places appropriate obligations on any third party / subcontractor to ensure that our own obligations to our clients are fulfilled.

INFORMATION SECURITY & TECHNICAL AND ORGANISATIONAL MEASURES

QMS take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including:

- Restriction of access to a 'need to know' only basis
- Role Based Access Controls
- Secure password policy
- Encryption of data during transit to NHS standards
- Anonymisation processes in line with ICO guidance
- Secure HSCN hosting of patient confidential data

QMS PROCESSING SAFEGUARDS

For all our client services, QMS will ensure the following safeguards:

PROCESSING TO MEET THE REQUIREMENTS OF GDPR AND CONTROLLER/PROCESSOR CONTRACT

- QMS adheres to all current legislation including Duty of Common Law, Data Protection Act, and GDPR.
- QMS has rigorous internal processes in relation to Information Governance and maintains compliance with the Data Security and Protection Toolkit (DSPT), which is reviewed annually.
- QMS will only process data as defined by the Client Contract and will only process Personal Data on the client's documented instructions.
- QMS will return or securely destroy confidential personal data in an appropriate manner as defined by our processing agreements.

DEMONSTRATING COMPLIANCE

- QMS maintains a log of all data processing activities in line with guidance from the Information Commissioner's office. This is updated regularly in line with current legislation including Data Protection and GDPR.
- QMS will agree Data Protection Impact Assessment (DPIA) with Clients to assess and mitigate against any identified risks for all services.
- QMS will support clients to document their own compliance with regulations -for example assisting with Client DPIA and Privacy Notices for each service.

- QMS provide all staff with ongoing training in Information Governance, Data Protection, and this now includes GDPR.
- QMS will impose a duty of confidentiality on all staff with access to Personal Data, and ensure all staff understand all relevant responsibilities in relation to Data Protection and GDPR.

SECURITY

- QMS implement appropriate technical and organisational security measures, in line with current Information Governance guidance, including GDPR, and industry best practice. These are regularly reviewed.
- QMS risk assess our data processing activities in conjunction with QMS Clinical Risk Safety Officer and Data Protection Officer, and we mitigate appropriately where risks are identified.
- QMS regularly review these security measures, all staff receive appropriate training, including Cyber security, and our web applications are tested via external Penetration tests.
- QMS will return or delete all Personal Data at the end of our relationship with the client, as detailed in the contract.
- QMS has assigned responsibility for GDPR to a nominated Data Protection Officer.
- QMS will continue to implement appropriate technical and organisational security measures, with regular review of these.

RESTRICTIONS ON SUBCONTRACTING

- QMS will ensure any sub-contractors we engage for the purposes of processing Personal Data are required to meet the requirements of the GDPR and any other standards we have agreed with clients in writing.

TRANSFER OUTSIDE THE EU

- QMS will not transfer Personal Data outside the UK.

SUPPORTING CLIENT GDPR OBLIGATIONS

- QMS will assist clients in meeting their own GDPR obligations (for example in relation to Privacy by design, Data Protection Impact Assessments, Privacy Notices and notification of breaches).
- QMS will make available all relevant information reasonably requested by the client and any competent regulatory authority to demonstrate QMS GDPR compliance.
- QMS will inform the client if, in our opinion, processing of a request for information violates the GDPR or other relevant data protection requirement.
- QMS will assist clients in responding to requests from Data Subject to exercise their rights under GDPR.

BREACH NOTIFICATION

- We will notify the client promptly in the event of any material security breach impacting Personal Data and will provide all reasonable assistance for breach investigations, mitigation and remediation.

GDPR ROLES AND EMPLOYEES

QMS have a designated Data Protection Officer (DPO) and QMS senior management are committed and engaged in complying with data protection regulations. The DPO is responsible for promoting awareness of the

GDPR across the organisation, assessing our GDPR compliance, identifying any gaps and approving and implementing policies, procedures and measures in relation to Data Protection.

QMS understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and maintain an employee training program to support this, including induction and annual refresher training.

If you have any questions in relation to Data Protection or GDPR, please contact dataprotection@qms-uk.com .