eConsult Health Ltd
GDPR and Data Protection and Information Security Compliance Statement

Introduction

eConsult Health Ltd (eConsult) takes the security and protection of personal data very seriously. We are committed to providing a compliant approach to data protection. We have always had a robust data protection and information security program in place which complies with existing law and abides by the data protection principles. We reviewed this program to ensure that it met the requirements of the EU General Data Protection Regulation ("GDPR") which came into force on 25 May 2018 and reviewed it once again when the UK left the EU. It is reviewed on an annual basis or whenever there is a legislative change.

The EU GDPR is an EU Regulation, and, as such, it no longer applies to the UK. eConsult operates inside the UK, hence needs to comply with the Data Protection Act 2018 (DPA 2018).

The main provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR which sits alongside the DPA 2018. In practice, there is little change to the core data protection principles, rights and obligations. GDPR recitals add depth and help to explain the binding articles. Recitals continue to have the same status as before – they are not legally binding; they are useful for understanding the meaning of the articles.

When we process any personal data, we will do so according to the data processing principles of the GDPR defined in this legislation. For the purposes of this statement, the above will be referred to as 'GDPR'.

Our Commitment

eConsult Health Ltd *('we' or 'us' or 'our')* are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We recognise our obligations in continuously updating, expanding and reviewing this program to meet the demands of the GDPR as use the ICO Accountability Framework as our guidance and metrics to measure against.

eConsult are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of the GDPR. Our objectives for GDPR compliance summarised in this statement and data protection roles, policies, procedures, controls and measures to ensure ongoing compliance.

How We Are Meeting GDPR

Information Audit - we carried out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

Policies & Procedures - we updated and implemented new data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including:

- **Data Protection** – our Information Security and Data Protection Policy has been reviewed to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to

ensure that we understand and adequately disseminate and evidence our obligations and responsibilities.

- **Data Retention & Erasure**– we have introduced a data retention policy to ensure that we meet the 'data minimisation' and 'storage limitation' principles and that personal information is stored, archived and destroyed in accordance with our obligations under the GDPR. We have erasure procedures in place to meet the 'Right to Erasure' obligation and are aware of when this and other data subject's rights apply, along with any exemptions, response timeframes and notification responsibilities.
- **Data Breaches**– our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate, and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
- **International Data Transfers & Third-Party Disclosures** – where eConsult stores or transfers personal information outside the UK or EU, we have procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data as appropriate. Our procedures include a regular review of the countries with sufficient adequacy decisions; standard data protection clauses for those countries without. We carry out due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.
- **Subject Access Request (SAR)** – we have revised our SAR procedures to accommodate the 30-day timeframe for providing the requested information and for making this provision free of charge.

Legal Basis for Processing - we reviewed all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR are met.

Privacy Notice/Policy– we have revised our Privacy Notices to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.

Obtaining Consent - we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information, together with clear instructions on how to withdraw consent at any time.

Data Protection Impact Assessments (DPIA) – where we process personal information that is considered high risk, involves large scale processing, or includes special category/criminal conviction data, we have developed procedures for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

Processor Agreements – where we use any third party to process personal information on our behalf (e.g., Payroll, Recruitment, Hosting etc.), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they meet and understand our mutual GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.

Special Categories Data – where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements (and have high-level encryptions and protections on all such data). Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis. (Where we rely on consent for processing, this is explicit, with the right to modify or remove consent being clearly signposted.)

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information in our Privacy Policy regarding an individual's right to access personal information that eConsult processes about them and to request information about:

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store their personal data
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances.

Information Security & Technical and Organisational Measures

eConsult takes the privacy and security of individuals and their personal information very seriously and 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:

Physical and Environmental Security

- Physical security controls, specific to buildings, on the perimeter of all of our premises in order to protect the systems and information within. Physical security is reassessed annually and any required improvements or additions to the current systems implemented.
- Entry to eConsult's premises is controlled through use of key cards.
- Office access is restricted to authorised personnel and escorted visitors only within working hours. IT Systems and related equipment are stored in locked rooms with access restricted to minimum personnel required.
- Potential threats from environmental factors such as fire and flood are reviewed annually, and fire alarms are installed in premises.
- All computer infrastructure is hosted within ISO 27001 certified data centres, access to which is limited to authorised personnel on a business needs basis. It is supported by sufficient utilities including back-ups.
- Equipment is disposed of securely, with hard drives and other items wiped, with certificates of destruction obtained where appropriate.
- eConsult has ISO 27001 certification obtained from Alcumus ISOQAR (see certificate below).

Alcumus ISOQAR

Certificate of Registration

This is to certify that the Management System of:

eConsult Health Limited

3rd Floor, Moorfoot House, 221 Marsh Wall, London, E14 9FJ

has been approved by Alcumus ISOQAR and is compliant with the requirements of:

ISO 27001: 2013

ISOQAR UKAS MANAGEMENT SYSTEMS 0026

Certificate Number:	**20623-ISMS-001**
Initial Registration Date:	07/12/2021
Expiry Date:	07/12/2024

Scope of Registration:

The provision of software developed medical and digital health products including the company-wide IT security management processes for operations, development and support services offered through implementation in accordance with SOA Version 1, dated 3/12/2021

Signed:
Alyn Franklin, Chief Executive Officer
(on behalf of Alcumus ISOQAR)

Alyn Franklin

Operations Management

- All systems have documented operating procedures, including but not limited to:
  - Backup
  - User Administration
  - Monitoring of Logs
  - Error Handling
- Change Management of systems is formally documented and reviewed.

- Segregation of duties is practised to ensure that accidental or deliberate misuse is minimised.
- Third Party service agreements have agreed service delivery levels which are monitored and recorded internally. Issues are raised by the relevant manager or the Head of IT to the third party immediately.

System Planning

System capacities are reviewed regularly, including whenever a new system is implemented, to ensure continued smooth running of all systems and minimise risk of failures.

System Protection

- All systems are protected from malicious and unauthorised software
- Anti-virus software is installed on all computers, IT systems and gateway, and updated automatically
- All email undergoes anti-virus scanning before being relayed to users
- All media undergoes anti-virus scanning before use
- Users do not have permission to run or install programmes that are not authorised by IT - only administrators have permission to install applications on machines.

Back Ups

- All IT systems are backed up daily (or more frequently in the case of patient facing production systems) and the backups checked for success
- Backup recovery is tested at least monthly
- Backups are taken before any major system.

Enterprise Security Management

- Appropriate security controls are implemented across the enterprise to ensure the ongoing security of in terms of confidentiality, integrity and availability. The enterprise is protected by a secure firewall.
- All internet and email traffic is scanned before being accessed by internal resources. Networks are segregated into defined areas to ensure that people only have access to the areas necessary and to minimise the impact of an attack.
- Networks are actively managed, monitored and checked to ensure that only authorised equipment, services and software are residing and using the network.

Monitoring

- To ensure there are no unauthorised information processing activities, logs are maintained of all user and administrator activities, kept for a minimum of six months and are subject to back-ups
- Logs are regularly monitored and automated alerts are configured for security events or suspected breaches. Internet activity is monitored and reports regularly sent to line management

Access Control

- Access is given on a need only basis and a minimum level of access is provided for the user/administrator to carry out their role
- All access is authorised by a manager
- Administrators have a separate user and administrator account
- The user account is to be used for “day-to-day” work e.g. email, and the Administrator account is used for administrator tasks only
- The Administrator account is not used for browsing the internet
- User Groups are defined according to departments and roles, restricting user access to the minimum services required.

User Access Management

- Users are only granted access to systems once the appropriate request has been submitted and approved
- Privileges are only granted once permission has been granted. Initial passwords are changed, and shared passwords prohibited
- User access rights are regularly reviewed
- User responsibilities are set out in the Acceptable use policy, which provides guidance on password setting and cyber-security best practice
- All staff undergo IT security training

Network Access

- Users only have access to systems that they are explicitly permitted and trained to use
- Any connections by remote users to systems are controlled through:
    - Use of authorised equipment, encrypted channels and a challenge/response protocol for remote access to the network.
    - Only authorised equipment and nodes are used on the network.
    - Ports are locked down or turned off.
    - Networks are segregated into defined areas to control access and information flow around the network.
    - All internet and email traffic is scanned before being accessed by internal resources.
    - All connections and access to the network are authenticated and authorised.

Operating System Access

- To prevent unauthorised access to operating systems the following policies are in place:
- Secure Log-On Procedures -all users logon to the network prior to getting access to any resources and are reminded to abide by the Information Security Policy and supporting procedures and that their activity is subject to monitoring and recording.
- User Identification & Authorisation - all users have a unique ID for logon to the system. All administrators have a separate unique ID for logging onto an administration account. Shared administration accounts are not used. Remote access by users is via two factor authentication or via username and password if they are only accessing email.
- Password Management System -all passwords are managed through designated administrators; settings are configured in line with the requirements of the Password Usage guidance. All default passwords are changed on installation of hardware or software. Any shared passwords are stored in a password safe and any access to this is recorded.
- Use of System Utilities -restricted to administrators only. Users do not have the ability to install programs and have a locked down build which does not allow access to utilities such as Command Prompt.

Application and Information Access Control

- Information Access Restriction - access to systems and information is limited to the minimum number of people required by the business. Google Drive Groups are used to control access to network shares.
- Sensitive System Isolation - any systems that contain sensitive information e.g. HR are isolated so that only authorised people have access to it. Logical and physical segregation controls are in place.
- Mobile Computing -all mobile computing devices are protected when used outside office premises – encryption is enabled or installed on the devices and password protected.

Information Systems Acquisition, Development and Maintenance

- **Security Requirements Analysis and Specification** - all new systems have their security requirements analysed during the requirements definition stage of the project including how information will be accessed, stored and transported, its impact on the other systems on the network, interconnections and any associated security requirements, maintenance and privacy by design.
- **Correct Processing in Applications**
  - Data input to applications is validated (automatically or manually) to ensure that it is correct and appropriate.
  - Message integrity techniques are used to check message authenticity. Digital signatures using commercially approved algorithms (e.g. RSA, SHA) are used to validate email authenticity.
  - Data output from applications is validated to ensure that it is correct and appropriate where required. These may be automated or manual validation.
- **Cryptographic Controls**
  - Commercially known, widely used cryptographic algorithms are used for encryption, including AES, RSA, SHA, DSA, with a certificate attesting to the correct implementation of cryptography (e.g. FIPS 140-2).
  - All information stored on media and mobile devices is encrypted.
  - Any sensitive information sent via email is encrypted.
  - All VPNs have encryption enabled.
  - Most cryptographic keys are managed by the commercial products however, there is often a master key or password which enables key recovery or “unlocks” the device. All keys are kept securely and offline within a fireproof safe. Access is limited to as few personnel as possible and all access/use is recorded.
- **Security of System Files**
  - Updates or changes to operational software is subject to a change control process.
  - All software is under vendor license agreements and operated according to the terms of these. Only authorised changes to operational software are permitted.
  - Any test data is protected on the test system in line with the sensitivity of the data. The test data is kept separate from live to reduce the risk of contamination. “Personal” data is not permitted to be test data unless it is anonymised prior to use.
  - All source code is securely stored in a source code repository and subject to quality control processes to ensure that only correct versions of source code are released. Access to source code is restricted to developers and necessary IT staff only.
- **Security in Development and Support Processes**
  - A change control process is in place and covers all aspects of changes to the system including changes in application system software. The change control process ensures that adequate testing of changes takes place.
  - All applications are reviewed after any changes to the operating system, including patches and service packs. All patches and service packs are tested prior to being applied and the applications are tested to ensure that they function correctly.
  - Changes to software packages are not made unless there is a business need. Any changes are governed by the change control process and undertaken as a new project. Changes are made by qualified personnel only.
  - All applications are tested for information leakage. Security test scripts are run on any developed software to check for common vulnerabilities such as buffer overflows. Software and applications are only procured from reputable sources.
  - Any software development that has been outsourced is subject to the same development controls as any software developed in house. The software is implemented under the change control process and security test scripts run in house.
- **Technical Vulnerability Management**
  - All systems are patched in a timely manner.
  - Patches are identified when they are released and tested and applied within 2 weeks of release.
  - Vulnerability websites are monitored to identify patches that will not be automatically downloaded.
  - Patches are applied to all applications and operating systems in use.

- A hardened operating system build that is in line with vendor guidelines is applied to all machines.

Information Security Incident Management

- **Reporting Information Security Events & Weaknesses**
  - All information security events are reported to managers and the SIRO immediately – staff are trained on the incident response process.
  - All information security weaknesses are reported to managers and the SIRO.

- **Management of Information Security**
  - All information security incidents are reported and logged via the IT Help Desk system. Events are classified dependent upon their severity. The log includes the ongoing handling and monitoring of the situation and any remedial or resultant corrective actions.
  - Incidents are handled, based upon their classification, and escalated to the information security committee. Responsibility for action taken in response to an information security event is with the company Founders and the Head of IT. The information security committee will review all incidents at regular committee meetings.
  - The Information Security Policy and other procedural documentation are reviewed following a security event and updated as appropriate.
  - Evidence is preserved to ensure that it can be reviewed and used against a person or organisation. In case of a serious offence, evidence is collected and preserved by experts to ensure any prosecution is successful.

- **Information Security Aspects of Business Continuity Management**
  - A business continuity policy is in place and tested at least annually to ensure that interruptions to business activities are minimised. The policy complements the incident management process to ensure that both are invoked (if appropriate) in the case of an information security incident.
  - Risk assessments take place to identify the likelihood of incidents occurring and to establish the priority in which services are recovered. They will cover all aspects and geographic locations.

GDPR Roles and Employees

eConsult have designated a Data Protection Officer (DPO) who works alongside the Information Security Group led by the Director of Information Security. The Information Security Group is responsible for promoting awareness of the GDPR across the organisation, assessing GDPR compliance, identifying any gap areas and implementing policies, procedures and measures. The Data Protection Officer supervises this work.

All employees, contractors and temporary members of staff undergo pre-employment checks as part of our onboarding procedure and are bound by confidentiality obligations.

eConsult understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have implemented an employee training program specific to the GDPR, which also forms part of our induction and annual training program.

If you have any questions about our standards, please contact the DPO