Kheiron Medical

Artificial Intelligence (AI) Data Protection Audit Report

March 2022

Executive summary

Background & Scope

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UKGDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

The ICO recognises that Artificial Intelligence (AI) offers opportunities that could bring marked improvements for society. But shifting the processing of personal data to these complex and sometimes opaque systems comes with inherent risks. The purpose of the audit is to provide the Information Commissioner and Kheiron Medical (KM) with an independent assurance of the extent to which the AI system, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of KM processing of personal data within the AI system. The ICO has further tailored the controls in scope to take into account the organisational structure of KM, the nature and extent of KM's processing of personal data within the AI system and whether KM is the developer, is providing AI as a service, or has procured the system for use in their organisation. As such, the scope of this audit is unique to KM.

It was agreed that the audit would focus on the following area(s):

- A: Governance
- B: Transparency
- C: Lawful Basis

- D: Contracts and 3rd Parties
- E: Data Minimisation
- F: Individual Rights
- G: Staff Training
- H: DP Risk Management
- I: Security and Integrity
- J: Trade Offs
- K: Statistical Accuracy
- L: Discrimination and Bias
- M: Human Review

Audits are conducted following the Information Commissioner's audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore KM agreed to conduct the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 7 March to 10 March. The ICO would like to thank KM for its flexibility and commitment to the audit during difficult and challenging circumstances.

Where weaknesses were identified recommendations have been made to promote compliance with data protection legislation. In order to assist KM in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. KM's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Overview of System and Data Processing

KM have developed the Mammography Intelligent Assessment (MIA) AI system. This system will work alongside radiologists as part of the mammography process, replacing one of the two radiologists who jointly make the decision of whether or not to recall a patient for further assessment, and so reducing the workload on radiologist services significantly. KM have used machine learning to train MIA to identify potential cancers in mammogram images, and have achieved an accuracy rate that is comparable to a trained radiologist. MIA is CE marked, which means it has been authorised for sale in the UK as a medical device by the Medicines and Healthcare products Regulatory Agency (MHRA).

Personal data is kept under the control of the healthcare authority responsible for the patient interaction, with KM functioning as a data processor, and is uploaded to MIA via an automated Gateway system. The data is pseudonymised within the Gateway hosted by the healthcare provider before transfer to MIA in order to reduce the risk of processing. The mammography assessment results from MIA are transferred back to the Gateway where the data is reconciled and written back to the patient record in the healthcare authorities own systems via the MIA Gateway. Similarly when KM receives data from healthcare authorities in order to use for machine learning purposes, this data is pseudonymised before transfer to KM systems, and in this instance KM act as Joint Controller for the data alongside the providing healthcare authority.

Due to the nature of the training data available, there are some limits on the populations for whom MIA can be used. KM demonstrated that they are aware of these limits, and factor them into the system documentation provided to healthcare partners for using the system. These include limits on age groups, with the system not having been trained on under 18s for example.

KM have an extensive level of governance and documentation in place, managed through the Greenlight Guru quality management system. KM are certified to ISO 27001 (information security), as well as ISO 13485 (quality management for medical devices), and are pursuing a Cyber Essentials Plus certification in the near future. On top of this the medical device regulations in the markets that KM operate in (UK, EU, and USA in particular) have very strict regulatory oversight, so KM have frequent engagement with medical device regulators to ensure MIA continues to operate in the way that was originally authorised by those regulators.

Audit Summary

Domains	Assurance Rating	Overall Opinion
Governance Transparency Lawful Basis Contracts & 3rd Parties Data Minimisation Staff Training DP Risk Management Security and Integrity Trade Offs Statistical Accuracy Discrimination & Bias Human Review	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.
Individual Rights	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

Areas for Improvement

- Kheiron Medical should develop a Record of Processing Activity that is fully compliant with the requirements of Article 30 of the UKGDPR.
- Kheiron Medical should fully document their process for handling individual rights requests.

Best Practice

Due to their experience of working in a highly regulated environment, KM have an extremely strong data and privacy governance process in place, with high levels of documentation and clear audit trails for all decisions and processes. This ensured the audit engagement ran smoothly and also facilitated KM's demonstration of compliance with legislative requirements, in particular those of Article 5(2) of the UKGDPR.

In addition it was noted that there is a clear and very positive data subject-centric attitude to the use of personal data, prioritising the preservation of the data subject's security and rights at every stage of the development and commercialisation process.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the engagement and are not necessarily a comprehensive statement of all the areas requiring improvement. The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Kheiron Medical.

We take all reasonable care to ensure that our report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is solely for the use of Kheiron Medical. The scope areas and controls covered have been tailored to this engagement and, as a result, the report is not intended to be used in comparison with other ICO report