Access Matters: Cloud Computing Policy

1. Purpose

1.1 This note provides guidelines for researchers and their use of cloud computing services for the storage and processing of UK Biobank data. It sets out UK Biobank's:

1.1.1 general perspective on cloud computing services; and

1.1.2 expectations for the management and protection of UK Biobank data when using cloud computing services.

1.2 Cloud computing, as defined by the National Institute for Standards and Technology (NIST)[1], is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

1.3 Although UK Biobank de-identifies participant data prior to its release to researchers[2], these data still contain clinical information and must be protected. Participant-level data will only be released by UK Biobank to researchers (whose application has been approved by UK Biobank) who agree to enter into UK Biobank's Material Transfer Agreement[3] which details what researchers are entitled to do with participant-level data.

2. General Perspectives

2.1 New computing paradigms continue to emerge that are generally useful to improving a researcher's ability to perform high quality research.

2.2 Cloud computing allows researchers to provision and make use of compute resource in more flexible, scalable and cost efficient ways and that ultimately will improve the quality of research undertaken and the value of results returned to UK Biobank.

2.3 In contrast to traditional computing undertaken on local servers and infrastructure directly owned and managed by a research organisation, cloud computing often entails the transfer and storage of data on systems managed by a third party. Security controls are required to protect against unauthorised access, data loss or theft, and these need to be proactively managed between a research organisation and their cloud computing provider.

2.4 UK Biobank treats information security of its data with the utmost concern. Participants have provided their data to UK Biobank secure in the knowledge that it will be safeguarded and only provided to bona fide researchers for health-related research that is in the public interest. No organisation or individual should have access to UK Biobank data outside the scope of an approved Access application that has been adjudicated in accordance with our Access Procedures.

2.5 As set out in our Access Procedures and specified within the Material Transfer Agreement, researchers are required to securely retain UK Biobank data at such standard as would be reasonably expected for the storage of sensitive/confidential/clinical data.

---

[1] The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, Peter Mell / Timothy Grance - http://dx.doi.org/10.6028/NIST.SP.800-145

[2] UK Biobank Summary De-Identification Protocol - http://www.ukbiobank.ac.uk/wp-content/uploads/2013/10/ukbiobank-summary-de-identification-protocol.pdf

[3] UK Biobank Material Transfer Agreement (Applicant PI) - http://www.ukbiobank.ac.uk/wp-content/uploads/2016/11/Applicant-MTA.pdf

3. Requirements for researchers and research organisations

3.1 UK Biobank is not seeking to advocate or recommend specific cloud computing providers and rather is providing guidance as to the controls that must be put in place by research organisations and open to scrutiny. As part of the terms of its Material Transfer Agreement, UK Biobank reserves the right to audit the Applicant in order to review the security, storage or other arrangements for UK Biobank materials provided.

3.2 Researchers are not required to seek authorisation for their intended use of cloud computing, as research organisations already have obligations as laid out in UK Biobank's Material Transfer Agreement that relate to the handling of UK Biobank data. However, research organisations must undertake sufficient due diligence (in advance) to ensure that any use of cloud computing services meet UK Biobank's requirements as well as their own IT security requirements and policies.

3.3 As such, UK Biobank does not consider a research organisation's intended use of cloud computing as being any different to their use of internal IT systems and that maintaining information security in cloud-delivered environments remains the responsibility of the research organisation, though the implementation of that security becomes a contracted task between the research organisation and cloud computing provider.

3.4 Any use of cloud computing must be covered by a contract agreed between the legal entity (which is the research organisation) and the cloud computing provider. On no account should UK Biobank data be stored or processed using 'personal' cloud computing services and where the agreement for use is between an individual and the cloud computing provider.

3.5 UK Biobank would expect that a research organisation's intended use of cloud computing services be reviewed by a senior representative of their internal IT organisation and who can certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing provider. UK Biobank holds the research organisation fully responsible for any failure in oversight of using cloud computing services for storing or processing UK Biobank data.

3.6 Where such services are used, research organisations are required to ensure individual researchers have their own access credentials that are not shared with others. Access by individual researchers must be fully auditable and limited to only those approved as part of the Applicant application.

3.7 UK Biobank expects a minimum set of controls to be in place at the research organisation, based on a security in-depth model, that includes (but is not limited to):

- 3.7.1 preventing unauthorised access and sharing;
- 3.7.2 monitoring and audit of the infrastructure and employee access;
- 3.7.3 encryption of data both at rest and in transit (AES256 recommended);
- 3.7.4 conducting regular risk/vulnerability assessment and analysis.

3.8 Research organisations should familiarise themselves with the security capabilities of their chosen cloud computing services provider and be confident that services provided can be considered as offering a secure network system.

3.9 The cloud computing provider must be able to offer verified evidence of third party audits to validate their information security controls and that these are externally audited on a regular basis. UK Biobank would expect any reputable cloud computing services provider to be certified to information security industry standards, including (but not limited to) ISO27001, ISO27017 and ISO27018.

3.10 UK Biobank would expect that direct employees of the cloud computing services provider with physical access to the network, storage and compute resource (for administration or maintenance purposes) have been vetted, and that the provider has taken steps to control and audit their access.

3.11 The cloud computing services provider must be able to specify the geographic location(s) where data are to be stored, and that this is contractually defined requirement between the research organisation and the provider.

3.12 The cloud computing services provider must be able to confirm how data will be securely deleted or destroyed, either at request of the research organisation or at the end of the service agreement, and that this is an auditable process.

3.13 Lastly, on no account should use of a cloud computing services provider convey any rights to the cloud computing provider itself for the access to or processing of UK Biobank data.