Date of policy: 28 June 2017

UK Health Forum Data Protection Policy

1. Purpose and objectives

This policy describes the UK Health Forum's (UKHF) commitment to the safeguarding of personal data processed[1] by its staff.

Its objectives are:

- To help staff recognise personal data
- To help them understand their rights and obligations with respect to personal data.

2. Introduction

The UKHF processes the personal data of living individuals such as its staff, contractors, research subjects, members and registered users. This processing is regulated by the Data Protection Act (DPA) 1998. The UK's regulator for the DPA is the Information Commissioner's Office.
It is the duty of the UKHF to comply with the data protection principles with respect to personal data (Appendix A).

This policy describes how the UKHF will comply with the DPA in general and the data protection principles and rights of data subjects.

3. Roles and responsibilities

The Senior Management Team is responsible for defining UKHF's policies and for ensuring they are implemented by all staff through Heads of Departments.

The Data Controller at the UKHF with support from the Senior Management Team and the Board of Directors has primary responsibility for UKHF's compliance with the DPA.

The Data Protection Controller can be contacted:
helena.korjonen [at] ukhealthforum.org.uk

4. Security of personal data

All staff processing personal data should ensure that the data are secure and appropriate measures must be taken to prevent unauthorised access, disclosure and loss. Staff whose work includes

[1] includes activities such as creating, storing, consulting, amending, disclosing and destroying data

responsibility for supervision of contractors, or temporary staff, or students, have a duty to ensure that they observe the eight principles of the Act.

It is rarely necessary to store electronic personal data on portable devices such as laptops, USB flash drives, portable hard drives, CDs, DVDs, or any computer not owned by UKHF.

Similarly, manual personal data should not be regularly removed from UKHF premises. In the case of electronic data, to minimise the risk of loss or disclosure, a secure remote connection to UKHF should be used wherever possible.

Downloading personal data on to portable devices or taking manual personal data offsite must be authorised in writing by the Data Owner, who must explain and justify the operational need in relation to the volume and sensitivity of the data. The data must be strongly encrypted. Users should only store the data necessary for their immediate needs and should remove the data as soon as possible.

Manual personal data and portable electronic devices should be stored in locked units, and they should not be left on desks overnight or in view of third parties.

In order to comply with the fifth data protection principle personal data should be securely destroyed when no longer required, with consideration for the format of the data

Personal data must not be disclosed unlawfully to any third party. Transfers of personal data to third parties must be authorised in writing by the Data Owner and protected by adequate contractual provisions or data processor agreements, agree with the UKHF's notification and must use safe transport mechanisms.

All losses of personal data must be reported to the Senior Management Team. Negligent loss or unauthorised disclosure of personal data, or failure to report such events, may be treated as a disciplinary matter and could be considered gross misconduct.

Publication of staff information
The UKHF will make public as much corporate information as possible. The following types of personal information will usually be published:

- Names of members of the Board, the Senior Management Team and members of staff.
- Research expertise and achievements of staff.
- Annual audited and approved financial accounts.
- Members of the organisation.

5. Access to personal data

I seem to close this gap, to make it consistent with the other headers
Subject access rights
Data subjects have a right of access to their personal data, including some unstructured manual personal data. Subject access requests must be made in writing to the UKHF (email is fine).

DATA SUBJECTS MUST PROVE THEIR IDENTITY AT THE POINT OF REQUEST.

Copies of requested information will be provided in permanent form promptly and in any event within 40 days. In the case of requests made about funding or ongoing research projects, information will be provided where and when possible and after this has been cleared with the funders.

Some personal data are exempt from the right of subject access, including confidential references provided by the UKHF and research data.

UKHF DOES NOT CHARGE A FEE FOR SUBJECT ACCESS REQUESTS.

Although the DPA applies only to living individuals, data about deceased persons who at the time of processing would be under 100 years old should be treated as personal data.

6. Monitoring

It is sometimes necessary for the UKHF to monitor information and communications. This may include personal data. The circumstances in which monitoring may be carried out, and procedures for doing so, are described in the UKHF IT policies, staff contracts, evaluation frameworks and membership articles.

7. Third party access

In certain circumstances the DPA provides for disclosure of personal data, without the consent of the data subject, to certain organisations. Requests for such disclosures from third parties, such as the police, UK Border Agency, local authorities or sponsors, should be made in writing and handled by the UKHF Senior Management Team. This will ensure the validity of the request and any warrants or orders of court can be checked. Staff disclosing personal data may not be protected by an invalid warrant.

8. Records Management

Records in all formats containing personal data must be created, stored and disposed of in accordance with the UKHF's Corporate Policy and any associated procedures and codes of practice. They must be authentic, reliable and usable and capable of speedy and efficient retrieval. They must be retained for no longer than the periods permitted in UKHF's retention schedule and, when no longer required for operational reasons, must be transferred to UKHF's records storage facility or institutional archive (if selected for permanent preservation) or disposed of securely and confidentially.

9. Research using personal data

Personal data processed for research, statistical and historical purposes must not be used to support decisions with respect to data subjects or processed so as to cause them substantial damage or distress. Notwithstanding the fifth data protection principle, such data may be kept indefinitely. They may also be further processed for other research purposes and are exempt from the right of subject access as long as the results of the research do not identify data subjects.

Staff and students using personal data in research must:

- understand how personal data may be used in research
- use the minimum data necessary for the research, including, wherever possible, anonymised or pseudonymised data
- ensure their processing complies with all the data protection principles
- inform Senior Management Team or line manager about research before processing of personal data begins
- notify the UKHF Ethics Committee all research projects involving personal data before processing begins
- where relevant, inform data subjects about the purposes of the processing and ensure valid written consent is obtained
- ensure all personal data collected are necessary for the purpose(s) of the research
- keep the data securely
- ensure personal data are destroyed confidentially, stored with the Corporate Team or otherwise disposed of in compliance with agreements with funders.

10. Status

This document has been approved by the Senior Management Team and Board of Directors. It is a condition of employment that employees will abide by the regulations and policies made by UKHF. This policy will be reviewed and updated regularly.

Any questions or concerns about this policy, please contact:

helena. korjonen [at] ukhealthforum.org.uk

or

paul. lincoln [at] ukhealthforum.org.uk (Chief executive)

Appendix A: THE DATA PROTECTION PRINCIPLES

The data protection principles can be read on the Information Commissioners website:
https://ico.org.uk/for-organisations/guide-to-data-protection/

Information for the public can be found here:
https://ico.org.uk/for-the-public/