

# Global Healthcare Information Network/HIFA Privacy/Data Protection Policy

## 1. SCOPE

The policy applies to anybody whose personal data Global Healthcare Information Network processes. For these purposes, personal data means any information in any recorded form which, on its own or combined with other data we hold, could be used to identify a living individual. The General Data Protection Regulation (GDPR) expands the definition of personal data so that as well as text, images and location data, it now expressly includes online identifiers.

## 2. PURPOSE AND OVERVIEW

This policy explains the approach of Global Healthcare Information Network as a data controller and data processor.

### **Introduction**

1. The Global Healthcare Information Network (GHIN) has a mission to improve health worldwide. GHIN/HIFA does this by promoting communication, understanding and advocacy for global health and the translation of reliable knowledge into policy and practice. To achieve this mission, the staff, volunteers, and other stakeholders of GHIN/HIFA use data in many ways. Some of these data are considered personal data belonging to living individuals known as data subjects, including prospective, current and future students, staff, supporters and members of the public. We use a variety of personal data from information collected and filed in databases through to photographs.
2. The current Data Protection Act 1998 (DPA) was replaced on 25 May 2018 with the General Data Protection Regulation (GDPR), which was enshrined in UK law by a new act of parliament.
3. GHIN/HIFA is a data controller as defined in the DPA and the GDPR because it chooses how it collects and processes personal data of staff, volunteers and others.
4. GHIN/HIFA must only process personal data fairly, lawfully and securely – please see the data protection principles below for further information.
5. GHIN/HIFA is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data. Good practice in the field of data privacy is continually evolving, and this policy and its associated documents will be updated to reflect such change.
6. This policy explains in plain language GHIN/HIFA's expectations of itself, its staff and

volunteers, when GHIN/HIFA processes your data, or asks contractors to do so on its behalf.

### **Principles of data privacy relevant to this policy**

1. The GDPR sets out the following six principles of data protection that require personal data to be collected and used fairly, stored safely and not disclosed to any other person unlawfully:
  - a. Where we process personal data, we must do so lawfully, fairly and transparently (“**lawfulness, fairness and transparency**”);
  - b. We must only process personal data for clearly pre-specified lawful purposes, and we cannot process personal data for any other reasons (“**purpose limitation**”);
  - c. We must only collect enough personal data for the stated purpose – the data must be adequate, relevant and only the amount necessary for the purpose for which it is processed (“**data minimisation**”).
  - d. The personal data we collect must be accurate and where necessary kept up to date (“**accuracy**”).
  - e. We must not keep personal data for longer than is necessary for its stated purpose (“**storage limitation**”).
  - f. We must only process personal data in a manner that ensures appropriate security, which includes protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“**integrity and confidentiality**”).
2. Processing has a very wide definition in law. It includes obtaining or collecting, recording, holding, storing, organising, adapting, reformatting, cleaning, copying, transferring, combining, pseudonymising, anonymising, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.
3. GHIN/HIFA, where it is a data controller, remains responsible for the control of any personal data it has collected, even if later passed onto another organisation or stored on systems or devices owned by other organisations or individuals (including devices personally owned by members of staff).
4. The new law means that many more data protection breaches must now be reported to the Information Commissioner’s Office. Where a report is needed, we must do so no later than 72 hours after the breach is discovered.

## **3. POLICY**

### **GHIN/HIFA duties as Data Controller and Data Processor**

1. GHIN/HIFA is legally responsible for demonstrating compliance with the six data protection principles described at paragraph 11 above. GHIN/HIFA arranges mandatory training for staff and students to enable them to comply with the law too. If any member of GHIN/HIFA is found to have breached this policy deliberately, GHIN/HIFA may take disciplinary action against them, including immediate suspension of access to GHIN/HIFA facilities. In very serious cases, such people may face criminal investigation.

2. GHIN/HIFA keeps a record of its processing activities.

### **Information Management and Security**

3. All members of GHIN/HIFA who use personal data must ensure that they hold such data securely, and that it is not disclosed to any unauthorised third party in any way, including by accident. In particular:
  - a. any mobile devices used for GHIN/HIFA work must be encrypted and password protected, whether supplied by GHIN/HIFA or personally by the staff member or student;
  - b. USB sticks and removable storage must never be used unless they and/or the files on them are encrypted and password protected;
  - c. if cloud-based storage is needed, this must be on the School's One Drive.

### **Lawful Conditions for Processing**

4. GDPR has clarified that data controllers like GHIN/HIFA must take care to choose the most appropriate lawful basis for processing personal data. The potentially lawful reasons for processing data are:
  - a. consent by the data subject;
  - b. the processing is required due to a contract between the data controller and data subject;
  - c. the data controller is obliged by law to process the data;
  - d. processing is necessary to protect someone's vital interests (i.e. life or death situation)
  - e. the data controller must process the data to perform a task carried out in the public interest;
  - f. the data controller needs to process the data in pursuit of its the legitimate interests or the interests of a third party, and the processing does not interfere with the rights and freedoms of the data subject.
5. All processing of personal data carried out by GHIN/HIFA must meet one or more of the conditions above. In addition the processing of 'special categories' of personal data requires extra, more stringent, conditions to be met in accordance with Article 9 of the GDPR.
6. Legitimate Interest  
GHIN/HIFA uses various ways to achieve our mission and to support our objectives: we believe that people who share our values would love to know how to support us. We will process the personal information you have supplied to us to conduct and manage our work to enable us to give you the most appropriate information, service and products and provide the best and most secure experience. We may very occasionally contact you by post or telephone to further the aims and objectives of GHIN/HIFA/HIFA. We will make sure our communications are relevant to you, tailored to your interests. Remember, you can change the way you hear from us or withdraw your permission for us to process your personal details at any time, and/or remove all your details from our records, by contacting us: [admin@hif.org](mailto:admin@hif.org)
7. Where GHIN/HIFA relies upon consent, it will work to ensure that this meets the definition of a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or other clear affirmative action, signifies

agreement to the processing of personal data relating to him or her”. GHIN/HIFA will not rely upon silence, pre-ticked boxes or inactivity where it relies upon consent as the lawful basis for processing.

8. GHIN/HIFA will clarify with those whose consent is relied upon that they can withdraw their consent at any time.
9. **Public Members Directories.** HIFA maintains public directories of profiles of HIFA members who have given explicit permission for their profile to be added to the directory(ies). To update or remove a profile from the directory, please write to [admin@hifa.org](mailto:admin@hifa.org)
10. **HIFA Contacts.** The HIFA website contains brief profiles (name, organization, country of residence, professional interests) and photos of individual HIFA staff and volunteers who have specifically consented to this. To update or remove a profile from the directory, please write to [admin@hifa.org](mailto:admin@hifa.org)
11. **HIFA Forums.** The HIFA Forums are hosted by the Dgroups platform ([www.dgroups.info](http://www.dgroups.info)) and are subject to the Privacy Policy of Dgroups, which is compliant with the GDPR. The Privacy Policy of Dgroups is available here: <https://dgroups.org/terms>
12. **Google Analytics.** We use a tool called “Google Analytics” to collect information about use of this site. Google Analytics collects information such as how often users visit this site, what pages they visit when they do so, and what other sites they used prior to coming to this site. We use the information we get from Google Analytics only to improve this site. Google Analytics collects only the IP address assigned to you on the date you visit this site, rather than your name or other identifying information. We do not combine the information collected through the use of Google Analytics with personally identifiable information. Although Google Analytics plants a permanent cookie on your web browser to identify you as a unique user the next time you visit this site, the cookie cannot be used by anyone but Google. Google’s ability to use and share information collected by Google Analytics about your visits to this site is restricted by the Google Analytics Terms of Use (as amended for government websites) and the Google Privacy Policy. You can prevent Google Analytics from recognizing you on return visits to this site by disabling cookies on your browser.

### **Data Subject Rights**

13. Data subjects have express rights to access and correct personal information held about them by GHIN/HIFA. Subject access allows individuals to confirm the accuracy of personal data and check the lawfulness of processing, and to exercise rights of correction or objection if necessary. As part of the right to access data, individuals can reasonably request to see information that GHIN/HIFA holds about them.
14. GHIN/HIFA will respond within one month to all requests by data subjects for access to their personal data, which will normally be provided free of charge.
15. In addition to accessing their personal data held by GHIN/HIFA, data subjects have the following rights (some of which are not absolute rights):
  - a. Right to Object – the right to object to specific types of processing;
  - b. Right to be forgotten (erasure) – the right to have their data erased in certain

situations e.g. the data are no longer required for the stated purpose. Some exemptions apply. Individuals can ask the controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved.

- c. Right to challenge the basis for automated decision making and profiling – in practice this right is unlikely to apply because GHIN/HIFA does not automate decisions and profiling is restricted to what is lawfully necessary, e.g. to comply with immigration law.
- d. Right to Rectification – data subjects may ask GHIN/HIFA to rectify inaccuracies in personal data held about them.
- e. Right to Portability – in practice, this right will not apply as GHIN/HIFA does not collect data that would be provided to another higher education provider in an agreed standard form.

### **Data Sharing**

16. GHIN/HIFA will only share personal data with a third party or external data processor where lawfully permitted to do so. In particular, GHIN/HIFA will ensure that such data sharing:

- a. is lawful and fair to the data subjects concerned;
- b. fulfils a legal requirement or a contractual commitment with the data subject;
- c. is necessary to meet GHIN/HIFA's legitimate interests;
- d. is necessary for a public task that is core to GHIN/HIFA's public functions; or
- e. is based on the data subject's informed consent.

17. GHIN/HIFA must also be satisfied that the third party will meet all the requirements of GDPR particularly in terms of holding the information securely. It will ensure that other legal requirements are in place, including a written contract with the party receiving the personal data.

### **Transfers of Personal Data Outside the EEA**

18. Personal data can only be transferred out of the European Union under certain circumstances. The GDPR lists the factors that should be considered to ensure an adequate level of protection for the data and some exemptions under which the data can be exported. In many cases GHIN/HIFA will require consent of data subjects before personal information can be transferred out of the EEA.

19. Information held in cloud storage where the servers are located outside the EEA, and/or which are published on the internet must be considered to be an export of data outside the EEA. GHIN/HIFA's main cloud storage on One Drive is safe for the purposes of GDPR.

20. Third Party Links. This Web site may contain links to third party Web sites that are not controlled by the owners and management of GHIN/HIFA. These third party links are made available to you as a member of the relevant GHIN/HIFA service(s) and you agree to use these links at your own risk. Please be aware that GHIN/HIFA cannot be held responsible for the content of third party Web sites nor are we responsible for the privacy policy or practices of those third party Web sites.

### **Data Protection Impact Assessments and Data Protection by Design**

21. The new law requires GHIN/HIFA to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to personal data.

### **Personal Data Breach**

22. GHIN/HIFA is responsible for ensuring appropriate and proportionate security for the personal data that we hold. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. GHIN/HIFA makes every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions. Examples of personal data breaches include:
- a. loss or theft of data or equipment;
  - b. inappropriate access controls allowing unauthorised use;
  - c. equipment failure;
  - d. unauthorised disclosure (e.g. email sent to the incorrect recipient);
  - e. human error; and/or
  - f. hacking attack.
23. If a data protection breach occurs GHIN/HIFA is required in most circumstances to report this as soon as possible to the Information Commissioner's Office, and not later than 72 hours after becoming aware of it.
24. If you become aware of a data protection breach you must report it immediately.

### **Sanctions for non-compliance**

25. GHIN/HIFA could face fines for non-compliance with the GDPR.
26. All GHIN staff and volunteers are required to comply with this Data Protection Policy, its supporting guidance and the requirements specified in the GDPR. Any member of staff or volunteer who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy may be subject to disciplinary action. Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of GHIN/HIFA i.e. for their own purposes, which are outside the legitimate purposes of GHIN/HIFA.

### **Data Protection Office**

27. This policy will be reviewed regularly, and at least annually for the first two years in recognition of the developing law, guidance and good practice in the area of data protection. It will be reviewed through the Management Board.
28. In the first instance all enquiries or requests for further information or guidance relating to data protection should be addressed to [admin@hifa.org](mailto:admin@hifa.org)

18 July 2019