Division of Population Health Information Governance Policy

Overview

A robustly constructed Information Governance (IG) framework allows an organisation to ensure that information is processed in accordance with all applicable regulations and guidance, such as the General Data Protection Regulations (GDPR), the Human Rights Act and the NHS Caldicott principles. The framework details the requirements, standards and best practice according to which information should be handled. Information should be managed securely and efficiently, and appropriate policies, procedures and management accountability should underpin the principles of the IG framework.

The Division of Population Health's IG policy is predominantly concerned with the handling of information related to research projects and research participant data, particularly that which is personal, confidential or sensitive. All research projects handling personal data should have a data management plan (DMP) which should address data capture, integrity, confidentiality, retention, sharing and publication, as per the Research Data Management Policy.

It is the Division of Population Health's policy to store only the minimum personal data required to satisfy the purpose for which it is collected, i.e. only anonymised or pseudonymised data is collected and stored where feasible. All research involving human participants, personal data or human tissue must be reviewed via one of the routes outlined in the University of Sheffield Research Ethics Policy. In addition, individuals have a right to be fully informed about all aspects of a research project in which they may participate, outlined in The University of Sheffield Ethics Policy note 2. Additional important information about data processing and legal rights of research participants is available through the University's Privacy Notice.

IG within the Division of Population Health is under the direction of the Division of Population Health IG Lead; the Division of Population Health IG Committee takes responsibility for ensuring tasks and activities relating to IG are carried out. Current membership, Terms of Reference of the Committee and role descriptions of the members are available on the Division of Population Health IG webpage.

Definitions

Data: For the purposes of this Division of Population Health policy, data includes both information about research participants and documentation related to research work.

Data Protection Impact Assessment (DPIA): a structured approach to identifying the privacy risks associated with the processing of personal data and for implementing appropriate controls to manage those risks. Data Protection Impact Assessments | Governance and Management | The University of Sheffield

Data Security and Protection Toolkit (DSPT): An online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. This is completed by the Division of Population Health IG Committee in order to assess our IG policies and procedures against these standards. Project teams using the DSPT as their security assurance must pay particular attention to the Process for projects using the Data Security and Protection Toolkit (DSPT) as the security assurance.

General Data Protection Regulation (GDPR): The law created in the European Union (EU) to protect personal data. The Data Protection Act 2018 enacts GDPR into UK law. Since leaving the EU, 'UK GDPR' alongside the amended version of the DPA 2018 are in effect. Guide to the UK General Data Protection Regulation (UK GDPR) | ICO

Information assets: Information assets include all research generated data, whether personal, sensitive or otherwise, along with associated documentation, hardware, software and any systems used in the pursuit of research aims.

Information Asset Owner (IAO): is the member of the Division of Population Health staff (usually the Principal Investigator (PI)) responsible for ensuring that information assets are handled and managed appropriately. See Information Asset Owner (IAO) for Division of Population Health projects

Information incident: An information incident is a potential or actual breach of data confidentiality, security or information governance policy.

Members of the Division of Population Health: For the purpose of this policy members of the Division of Population Health include Honorary[1] and Visiting staff, secondees, students and external researchers holding Service Level Agreements with the Division as well as those on the University payroll.

Primary user: The member of the Division of Population Health to whom a device has been assigned. All members of the Division of Population Health are expected to be assigned a device (desktop PC or laptop). In cases where there is desk sharing it is assumed there will be one user who primarily uses the device, however others may use it from time to time. Where there is a need for pooled laptops, each laptop will have a 'device owner' who manages the pool and must be responsible for the security of the devices.

Risk-bearing data: Personal, sensitive or confidential data about individuals, or information that is otherwise sensitive (e.g. commercially or politically sensitive information). The loss of risk-bearing data could be detrimental both to any individuals who might be identified and to the University's reputation. Pseudonymised data, where names and other personal identifiers have been replaced by a unique code, are still considered risk-bearing. Simple removal of names, other direct identifiers and unique codes may not sufficiently anonymise data.

Secure Data Service (SDS): The Secure Data Service is a cloud computing platform operated by IT Services using RONIN and hosted within Amazon Web Service (AWS). This is a platform designed to provide a secure environment for researchers to process sensitive data of any kind, whilst also providing scalable computing power for those researchers. Currently the platform is ISO 27001 compliant, and holds its own DSPT (EE133872-SDS) accreditation. Secure Data Services policies are managed by IT Services and copies can be requested from secure-data-service-group@sheffield.ac.uk

Security assurance: Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organisational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved where necessary, to ensure that the specific security and business objectives of the organisation are met. This should be done in conjunction with other

[1] Where non ScHARR staff have access to data this should be via a service level agreement (SLA) or contract

business management processes. Security assurance is the framework used to assess these controls, e.g. DSPT.

University-managed devices: devices running YoYo or managed desktops, e.g. desktops and laptops.

Purpose

The purpose of this policy document is to ensure that members of the Division of Population Health understand their responsibilities in the management of research data and associated information assets.

Scope

Each member of the Division of Population Health should be familiar with the principles and practices outlined in this policy document. All research should be conducted in accordance with this policy.

Policy review and update

The IG Committee will undertake an annual review of the Division of Population Health's IG policy to ensure that it remains up to date and fit for purpose. The Committee will incorporate findings of any internal information incident investigations and requirements of external agencies into this process and update policies and practices as necessary.

Section 1: Training and compliance

Background

Each member of the Division of Population Health, whether or not they carry out research, is likely to come into contact with risk-bearing data. It is a requirement of employment that members of the division complete mandatory IG training, which will demonstrate their compliance.

The IG Committee will be responsible for the oversight of training needs with annual review to determine the overall scope and shape of that training.

Policy

New Starters

It is the responsibility of Section Managers to inform the Division of Population Health -DS (population-health-ds@sheffield.ac.uk) of any new starters.

Training

Each member of the Division of Population Health (including Honorary staff and PGRs) must complete the following University data security training courses: Information Management; Data Protection; Protecting Research Data; and Cyber Security (all available via myDevelopment), and the Division of Population Health Information Governance (available via the training portal). These should be completed either annually or as mandated by the University.

Where other users have access to risk-bearing data (e.g. collaborators on the project who are external to the University of Sheffield, undergraduate students, or postgraduate taught students), they must complete the Division of Population Health Information Governance course and the Cyber Security course (both available via the training portal). They may also be required to complete additional training to ensure compliance with any security assurances given to data providers, e.g. through the Data Protection and Security Toolkit (DPST), data sharing agreements or contracts.

Policy enforcement

Failure to undertake appropriate IG training will result in suspension of access to University services (email, Google drive, calendar and Networked filestore folders).

Each member of the Division of Population Health should be aware that failure to abide by the Division of Population Health's IG policies may result in disciplinary action being taken against them.

Any infractions to policy will be added to the incident log, discussed with senior management, and handled in accordance with Section 6 (Incident Management).

Section 2: Information assets management

Background

It is the duty of the Division, through its IG management processes and structure, to be aware of and safeguard the information assets it possesses. The primary objective is to ensure that, in the event of damage, destruction, loss or theft, there is awareness of what information is affected and, in the case of loss or theft, whether the information held on the asset is protected from unauthorised access.

Policy

Each member of the Division of Population Health must manage all of their data in a way which satisfies legal and ethical obligations regarding patient confidentiality.

In practice there are three registers:

- a hardware inventory register, maintained by The Faculty IT Hub (foh-it@sheffield.ac.uk)
- a register of all projects maintained on the University's Shared Networked Filestore maintained by the Division of Population Health Data Security team (population-health-ds@sheffield.ac.uk), detailing the project name, folder location, information asset owner and deputies (IAOs), which users have access, and, if applicable, the expected archival/deletion date. IAOs are responsible for approving access for folder users. The leavers checklist is used to ensure access is removed when staff leave the Division of Population Health. See also the Routine maintenance of Division of Population Health resources on University Departmental Storage.
- a register containing details of all projects using the Data Security and Protection Toolkit (DSPT) as the security assurance, including project title, the information asset owner (usually the project lead), dates that the data sharing agreement is applicable between, details of data location, medium, and data destruction details. The IG Committee will keep the DSPT as a security assurance asset register up to date.

Device (hardware) management

All IT facilities (hardware, software, data, network access, third-party services, online services or IT credentials) provided or arranged by the University of Sheffield must be used in compliance with the University of Sheffield's IT Code of Practice.

It is expected that both personal and University-supplied portable devices (e.g. tablets and mobile phones) may be used off campus for work purposes with appropriate safeguards in place and subject to any other applicable agreement; refer to policy section 3 "Portable devices" and policy section 4 "Remote working".

Device users

University-owned devices

Any device purchased by the University is owned by the University.

Devices must not be used by individuals who are not members of the Division of Population Health unless under the direct supervision of a member of the Division of Population Health at all times (e.g. an external guest using a Division of Population Health computer to give a presentation to members of the division).
University-managed devices may be used by other members of the Division of Population Health, provided each user uses their own university account (e.g. where fully managed desktops, or YoYo desktops without privileged accounts are used for 'hot desking').
Under exceptional circumstances there may be devices which are university owned but not a YoYo or managed desktop; these must only be used by the individual to whom the device is assigned.
If the primary user of a University-owned device changes, the device must be reimaged and the Faculty IT Hub must be informed in order to update the hardware inventory register.

Non-University devices

See policy section 4 “Remote working”.

Device disposal/primary user leaves Division of Population Health

University-owned devices

Once University equipment is assessed by the Faculty IT Hub as having reached the end of its working life, suitable arrangements must be made for secure disposal and the asset register updated
See also the Division of Population Health Equipment Disposal and Reallocation Procedure.

Personal devices

Before disposing of, or providing access to, personal devices which have ever been used for University work/study purposes, or upon ceasing to be a member of the Division of Population Health, individuals must ensure:

- all risk-bearing data (if any) has been securely erased[2]
- all access to University systems has been removed and there is no access to the University Google account
- credentials relating to University systems have been securely erased (e.g. login details; VPN connection settings, etc.).

A “factory reset” is strongly recommended.

[2] It is contrary to policy to store risk-bearing data on personal devices

Section 3: Data storage and storage devices

Background

The Division of Population Health stores large volumes of research data, some of which is risk-bearing. The wrong choice of storage could put this data at risk of unauthorised access or loss and could damage the University's reputation.

In order to choose appropriate storage the following issues should be considered:

- **security** - ensuring that data is protected from unauthorised access. This is particularly important when working with risk-bearing data
- **availability** - ensuring that data is accessible when and where it is needed
- **integrity** - ensuring one true copy of the data is maintained.

Policy

Data from each research project should be stored in accordance with the agreements under which it has been collected or provided. It is the responsibility of the Information Asset Owner (IAO) to ensure all processes and agreements are adhered to, see Information Asset Owner (IAO) policy for further guidance.

It is recommended that risk-bearing data are stored in an access restricted folder on the University's Shared Networked Filestore, a UoS research virtual machine, or on the Secure Data Service (SDS). Where this is not practical, alternative or additional secure data storage must be chosen based on an assessment of potential risk. Advice must be sought from the relevant Section IG Lead.

Recommended storage

Shared Network Filestore

The Division of Population Health Data Security Team (DS) will create secure folders with controlled access and arrange archive or deletion on request. This will be documented in an information asset register (see Section 2).

For each project folder, research groups must only request access for those individuals who have a definite need for access to the contents of that folder. There is provision for secure access for people outside of the University when necessary. The IAO must notify Division of Population Health DS promptly when a member of staff no longer needs access. See Management of Division of Population Health Resources for further details.

IT Services manage the regular backup of all University file storage for disaster recovery purposes.

Virtual Machine (VM) and UoS Secure Data Service (SDS)

These are managed by IT Services, it is important to notify IT Services that the storage must adhere to the requirements of the Division of Population Health IG policy.

Other storage

Google Drive

The University has an agreement with Google for provision ofGoogle Workplace Apps, and are satisfied that the security controls put in place by Google are sufficient to protect University data. This applies only to University-supplied Google accounts and not to personal ones.

Google Drive must not be used to store data that relies on the DSPT as the security assurance.

Google Drive may be used by research groups as a tool to develop documents and spreadsheets collaboratively. However, it is not recommended for data storage for a number of reasons:

- when a Google account is deleted any documents owned by that account are also deleted unless they are first transferred to another account
- back-up and disaster recovery procedures are managed by Google and are therefore not within the control of IT Services
- there is increased risk of accidentally sharing data inappropriately
- users might have granted third-party applications access to files within Google Drive which may not have been formally assessed by UoS IT services
- using Google Filestream (which is endorsed in University guidance) could lead to files stored on Google Drive being copied onto a local machine (which would not be compliant with the Division of Population Health IG policy).

For these reasons Google Drive should not be used for risk-bearing data without very careful consideration of risks, and consultation with and approval from the appropriate Section IG Lead. When making these decisions consideration must be given to the regulatory (GDPR) requirements to maintain an asset register (see Section 2) and to monitor access and training. Specific processes would need to be put in place: to document granting and removal of access; to ensure files are only accessible to individuals who have completed the relevant training; to ensure access is removed when individuals leave the organisation; to document the expected archival/deletion date; and to inform the Section IG Lead where this information is maintained in order to be referenced by the register (see Section 2) of all projects which must be maintained by the Division of Population Health.

If a decision is made to collect or store risk-bearing data using Google Drive, e.g. via Google Forms, then this should be made clear to research participants.

High Performance Computing (HPC)

As part of its research computing provision, IT Services offer high performance computing services (e.g. Stanage and Bessemer) for work requiring intensive computational resources. These should not be used for processing risk-bearing data without first consulting the Division of Population Health IG Section Lead.

External services

External services should only be used for storage or processing of risk-bearing data following very careful consideration of risks and formal agreement by the IG Section Lead.

Examples of external service providers include:

- cloud storage services such as Dropbox, iCloud, OneDrive and Google Drive on personal (non-University) Google accounts
- online survey services such as SurveyMonkey (and Google Forms on non-University Google accounts)
- chat and video conferencing services (e.g. Slack, Zoom)
- agencies which process data (eg mailing, transcription)
- agencies which develop/maintain IT systems to support research projects
- software version control software (e.g. Git)

If a research group is considering using an external service for something which involves the processing or storage of risk-bearing data, they must consult the IG Section Lead for advice. If it is agreed that the use of an external service is appropriate, a contract must be in place to ensure there are sufficient security measures and compliance with the General Data Protection Regulations (GDPR). This is also likely to require the completion of a Data Protection Impact Assessment (DPIA).

Portable devices

Portable devices (e.g. laptops, USB sticks, hard drives, voice recorders, mobile phones, tablets) should only be used for *temporary* storage of data (and only where this does not violate any data sharing agreement) as they are vulnerable to loss or corruption. **All** portable devices (including personal mobile phones) **must** be encrypted if used for work purposes, including for receiving work emails or accessing the work calendar.

Data from third party providers

- There may be further restrictions placed on data received from third party providers.

Data sharing agreements (DSA) and/or contracts with these third party providers will document any restrictions.

Data Security and Protection Toolkit (DSPT)

If projects rely on the DSPT as the security assurance (e.g. DSPT has been referenced in the project's ethics application or within a data sharing agreement), the IG Section Lead must be informed so that details can be logged on the DSPT as a security assurance asset register.

DSPT assured data must never be stored anywhere other than in the approved location, which will usually be an access restricted project folder on the University's Shared Networked Filestore ("X drive" folder), in the Shared Networked Filestore allocated to the VM, or on storage provided on the SDS. See Process for using the DSPT as the security assurance.

Data Sharing Agreements (DSAs)

Any DSA with an external body must be approved by an authorised signatory in Research Services. Requests should be directed to ri-contracts@sheffield.ac.uk for review and approval (see section 5).

Audio/video recordings

Audio and/or video recordings should only be made on dedicated encrypted recording devices or as specified in the “Remote audio/video recordings” section, below. Alternative means of recording should only be used for research work following careful consideration of risks and consultation with the Section IG Lead.

Remote audio/video recordings

Division of Population Health staff/students may make audio/video recordings using Google Meet services under contract to the University of Sheffield (i.e. they must use their University accounts only) subject to the following general and service-specific conditions:

General conditions

Before making any recording, staff/students making recordings MUST ensure:

- their PC or laptop conforms to the Division of Population Health IG policy
- they make participants aware that the security of the participants'/interviewees' device is the participant's responsibility and if they are concerned they should not say anything they would not otherwise say while using their device/phone
- meetings contain only the participant(s) expected, with special regard to telephone participants whose identities may be more difficult to verify
- they do not inappropriately/inadvertently share the resulting recording(s)
- they, as soon as practicable, move the resulting recording(s) to a suitable longer-term storage location for “risk-bearing data” whilst observing the usual safeguards to ensure data is protected (see Section 3: Data storage and storage devices)
- they permanently delete the original recording(s) and do not seek to recover them

Specific conditions

Before making any recording, staff/students making recordings MUST ensure:

- they have not granted any unapproved third-party (non- GoogleWorkplace) apps access to their university Google Drive account (see https://myaccount.google.com/permissions)
- they do not "sync" or "stream" the contents of their university Google Drive account to any devices that do not conform with the Division of Population Health IG policy

Additional guidance on using Google Meet:

Knowledge base article on Google Meet - Virtual Meetings

Data disposal

The disposal of risk-bearing data requires particular care. Files which have been deleted in the usual way may still be recoverable; instead files containing risk-bearing data must be securely erased. Division of Population Health DS & the SDS team can provide the relevant technical assistance for the storage you are using.

The retention period for research data is determined by guidance from regulators, funders, sponsors and data providers, which must be adhered to. The retention period must be clearly defined within the ethics application and data management plan. The University of Sheffield records retention schedule can provide guidance if no other guidance is available. The IAO must ensure risk-bearing data is securely destroyed at the end of the retention period. If risk-bearing data is not destroyed by the end of the retention period this will be logged as an incident (see Section 6).

See also the data destruction process.

Paper records

Research project staff should discuss their requirements with their Section Manager to ensure paper records are stored securely and archived/deleted when appropriate. Where necessary, the Section Manager will consult with the Records Management Team.

Information captured on paper is just as important as data stored digitally and carries many of the same risks, therefore care must be taken to ensure secure transit of anything containing risk-bearing information.

Section 4: Remote working and working on devices which are not University-managed

Background

Working away from University premises and/or with devices which are not University-managed introduces additional risks, for example devices may be lost, damaged or stolen. Without appropriate protection this could result in the loss or inappropriate disclosure of risk-bearing data. Each member of the Division of Population Health has a responsibility to protect risk-bearing information and the systems they use to store, process or access that information and should be aware of the risks involved and take measures to safeguard this information. Losses of confidential data are viewed very seriously by the Information Commissioner's Office and the University, and may result in disciplinary procedures, civil court actions and criminal charges.

Policy

It is expected that most staff, the majority of the time, will work within the University environment (e.g. not downloading data locally, but connecting to University systems and storage via a VPN or 'direct access') on University-managed devices. Working remotely | IT Services | Staff hub (sheffield.ac.uk)

Devices used to access risk-bearing data must meet the following minimum standards:

- the device must not be accessible to unauthorised users
- the device must run under a vendor-supported and up-to-date operating system with all security patches applied
- the device must have appropriate firewall rules enabled
- if using Windows, the device must run an up-to-date anti-virus application
- the device must be encrypted

When working off site take care that work on sensitive information cannot be overlooked. Be aware that use of public Wi-Fi (e.g. Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (Wi-Fi where no password is required to access it) could be unsafe and lead to unauthorised access of personal data.

There may be further restrictions placed on data supplied by third party providers, and data sharing agreements (DSA) must be adhered to in these cases.

More detailed guidance is provided in "Ensuring data security when working remotely".

Section 5: Information sharing

Background

Researchers may have cause to share data relating to research participants with other persons, researchers or organisations. Sharing individual participant data can advance clinical research and benefit patients, but any sharing of data must always be in accordance with the law, and must be authorised under the agreements that govern the use of the data.

Data sharing and transferring requests must be handled in accordance with the requirements of GDPR and other relevant guidance, e.g. the NHS Caldicott principles. A failure to safeguard information could result in legal action.

Each member of the Division of Population Health must at all times have great regard for the safeguarding of the research data in their possession. Smith et al (2015) provides useful background information and guidance on data sharing and anonymisation and this is the document on which this Division of Population Health policy is based. If a person is unsure as to what action they should take then they should, in the first instance, approach their Section IG Lead and discuss the matter with them.

This policy must be applied to all information sharing requests that are not already authorised. This includes requests from individuals and groups both inside and outside of the University. For sharing of data outside the European Economic Area (EEA), please also see Section 7. Where sharing is already pre-authorised, e.g. with external collaborators, the project documentation should cover the IG arrangements for the other institution(s).

Policy

There must be a clear purpose to share research data which is aligned with the purposes for which the data were collected. The project team should ensure a system is in place to review data access requests and only accept them if this is satisfied. Similarly, data should only be deposited with data repositories which follow these principles.

Consent must be sought from data subjects if it is appropriate and practicable to do so (although a lack of consent for sharing does not prohibit the sharing of data if Section 251 approval has been obtained).

It is recommended that the following (or similar) wording be included in consent forms: “I understand that the information collected about me may be used to support other research in the future, and may be shared anonymously with other researchers.” Other data providers may have their own preferred wording.

Individuals have the right to be informed about the collection and use of their personal data and must be provided with information including the purpose for processing their personal data, retention periods and who it will be shared with (i.e. ‘privacy information’). It is important that this privacy information includes information regarding how to ‘opt-out’; if using data from NHS organisations (using Section 251 approval), where direct identifiers will not be obtained, then this information will most likely be to direct potential participants to the national data opt-out policy. If collecting data directly from consented participants it should be included within the participant information sheet (PIS). The ethics application process should document how this privacy information will be shared. For data obtained from third parties, where Section 251 approval has been obtained, it is likely this information will be provided in the form of a privacy notice. If projects rely on the Data Security and Protection Toolkit (DSPT) as the security assurance (e.g. projects that require Section 251 approval), the IG Section Lead must be informed so that details can be logged on the DSPT as a security assurance asset register (see Section 2) and the privacy notice checked.

Authorisation to share the information must be in place: agreement should be made within the project team regarding who should authorise requests for data sharing and it is expected that this will be outlined in a data management plan. As a minimum this should be from the project lead, but may also include the sponsor and ethics committee. Roles and responsibilities should be included in the protocol and data management plan.

Data must be anonymised as far as possible prior to being shared. There may be a trade-off between privacy and data utility as it can be difficult to attain true anonymisation and it is difficult to predict the risk of re-identification through data linkage. Refer to the University's Research Ethics Policy Note no 4 and Specialist Research Ethics Guidance Paper (PRINCIPLES OF ANONYMITY, CONFIDENTIALITY AND DATA PROTECTION).

The recipient of information must agree to safeguard the security and confidentiality of risk-bearing data. Where the transfer is outside University of Sheffield an agreement must be in place as part of a contract or as a separate data sharing agreement (DSA). This should outline the purpose and security arrangements and should clearly define what data should be shared and with which organisations (these parameters should be consistent with any study documentation such as the study protocol). For sharing with external institutions The University is generally legal party to DSAs to ensure that legal liability rests with the institution, rather than an individual employee/student.

Any DSAs with external institutions must be approved by an authorised signatory in Research Services, and enquiries should be directed to ri-contracts@sheffield.ac.uk for template DSAs, review and approval.

It is the responsibility of the person receiving or sharing the data to ensure compliance with all the obligations of the agreement on behalf of the University. Therefore the person receiving or sharing the data should sign the document in acknowledgement of the terms and conditions as well as a member of the Research Services Contracts Team.

Risk-bearing data must be shared securely. Files must be encrypted before they are sent via e-mail or stored in locations other than the Shared Network Filestore.See guidance on how to encrypt files. Advice may be sought from the relevant Section IG Lead.

Section 6: Incident management

Background

Information incidents include cases where there is potential, as well as actual, loss of or damage to data.

In order to protect sensitive information and to comply with data protection legislation, it is vital that procedures are in place to report any potential breaches of data confidentiality and security, i.e. information incidents.

Examples of information incidents include:

- Failure to follow University or Division of Population Health IG policies or procedures
- Sharing usernames and passwords. This is a breach of Information Security and expressly forbidden by the University.
- Saving of usernames and passwords within web browsers of shared computers
- Reuse of usernames and passwords
- Computers that are not protected by a password or are left unlocked
- Incorrect storage (insecure, non compliant) of risk-bearing data
- Offices left unlocked, or doors held open
- Lost/stolen equipment containing risk-bearing data that are not appropriately protected
- Information stored on external services without the proper checks
- Information shared incorrectly, e.g. transmission of risk-bearing data unencrypted by email

It is expected that all potential incidents, even if no data loss occurred will be reported to and assessed by the IG Committee.

The guidance on reporting an incident for the Data Protection Regulation (GDPR) and Networks and Information Systems (NIS) Directive, will be used by the IG Committee to help assess potential incidents.

The University Information security incident policy and procedure | IT Services | The University of Sheffield and Reporting a data breach | Governance and Management | The University of Sheffield will be followed.

Policy

Risk assessment

The IG Committee will formally assess and document risks to information and the controls put in place to manage risk.

The IG Committee will work with the Research Ethics Committee (REC) to assess IG risk on projects considered by the School of Medicine and Population Health (SMPH) REC.

Incident reporting

Any suspected information incident must be reported to a Section IG Lead, the IG Manager or the Division IG Lead as soon as possible.

However Division of Population Health staff should be aware that:

- A potential breach of risk-bearing data should be reported to the Data Protection team (Reporting a data breach | Governance and Management | The University of Sheffield)
- If an information security incident has occurred report to IT Services (Information security incident policy and procedure | IT Services | The University of Sheffield)

If Division of Population Health staff become aware outside of normal working hours of an information security incident that involves a serious loss of risk-bearing data and/or damage to computer systems, they should report it to University Security on 0114 222 4085, as mandated in the Information Security Incident Policy and Procedure.

Once a member of the IG Committee are aware of a possible information incident they will:

1. If not already reported: immediately report to IT Services if it involves an information security incident (Information security incident policy and procedure | IT Services | The University of Sheffield)
2. If not already reported: immediately report to the Data Protection team if it involves a potential data breach (Reporting a data breach | Governance and Management | The University of Sheffield)
3. If illegal activity (for example, theft) is suspected, ensure University Security Services have been informed
4. Record the incident in the Division of Population Health Incident Investigation Log
5. Carry out an investigation to establish the details and assess the impact, including the nature of the incident, the type of data involved, the perceived sensitivity of the data and the number of people affected, and record the details in the incident log[3]
6. Document any corrective actions taken and preventative actions to be taken in order to attempt to prevent any recurrence of this type of incident

The Division of Population Health Incident Investigation Log should only be shared outside of the IG Committee at the discretion of the IG Lead, unless there is a legal requirement to do so.

Where an incident is assessed that it is likely that some harm has occurred and that the impact is (at least) minor the IG Lead should report this to the Data Protection team who will follow the processes set out in Reporting a data breach | Governance and Management | The University of Sheffield

[3] This assessment may involve other relevant staff, such as IT technicians if appropriate: it may be necessary to download, open, read, copy or move files in order to determine whether they contain risk-bearing data

Section 7: International data transfers

Background

In accordance with GDPR, any risk-bearing data may not be transferred to locations outside the European Economic Area (EEA) unless the receiving organisation is in a position to guarantee the security rights of the data subject to a satisfactory standard.

Policy

In addition to the considerations listed in Section 6:

- Prior to any data transfer outside the EEA the Section IG Lead must be consulted.
- Depending on the complexity of the case it may be necessary to seek more detailed advice from the University's Research Services or from the Information Commissioner's Office.
- If the recipient country is not on the list of approved destinations it may be necessary to draft specific contractual guarantees with respect to confidentiality[4]. This should be dealt with on a case-by-case basis.
- Data that has been anonymised, or subjected to strong pseudonymisation, and cannot be further processed to recover identifiable information, may usually be transferred to locations outside the EEA without restriction as GDPR does not apply.

Further information

Information Commissioner's Office

https://ico.org.uk/for-organisations/guide-to-data-protection/

UK approach to international data transfers - GOV.UK (www.gov.uk)

European Union Commission website pages dealing with international data transfers
https://ec.europa.eu/info/law/law-topic/data-protection_en

[4] UK list of adequacy decisions
https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation

Section 8: Data processing by third parties

Background

The need to maintain high standards of information processing and handling is not limited to employees of the University of Sheffield. The same duty of care must apply to any person undertaking work on behalf of the Division of Population Health.

Policy

A contract or data processing agreement must be in place detailing how the data will be processed by the third party. Any contract or data processing agreement with a third party must be approved by an authorised signatory in Research Services. Requests should be directed to ri-contracts@sheffield.ac.uk for review and approval (see section 5).

Revision history

Version 1 authorised by the Dean, 24/11/2014

Version 16-03-31 authorised by the ScHARR Information Governance Committee 31/03/2016

Version 17-03-31 authorised by the ScHARR Information Governance Committee 31/03/2017

Version 18-03-31 authorised by the ScHARR Information Governance Committee 31/03/2018

Version 19-03-31 authorised by the ScHARR Information Governance Committee 25/03/2019

Version 19-08-09 authorised by the ScHARR Information Governance Committee 09/08/2019

Version 20-04-30 authorised by the ScHARR Information Governance Committee 30/04/2020

Version 20-10-13 authorised by the ScHARR Information Governance Committee 13/10/2020

Version 21-05-25 authorised by the ScHARR Information Governance Committee 25/05/2021

Version 22-01-24 authorised by the ScHARR Information Governance Committee 24/01/2022

Version 22-06-24 authorised by the ScHARR Information Governance Committee 24/06/2022

Version 24-04-02 (authorised by the Division of Population Health Information Governance Committee 02/04/2024 (emails collected and documented)

Version 24-06-03 (this version) authorised by the Division of Population Health Information Governance Committee 03/06/2024

Date	Section	Summary of changes
25th March 2019	General	Minor updates added throughout the policy where more clarity was required.
	Overview	Added references to relevant university policies in overview regarding anonymisation, ethics and data management planning
		Risk-bearing data definition updated so as not to imply the inclusion of all unpublished research
	Section 1	Training section updated: ScHARR IG training is annual, Cyber Essentials Assured Computing training is mandatory for anyone who will have access to NHS digital data
	Section 3	Extra information regarding the impact of using Google Drive rather than University network storage on existing procedures added.
		Extra subsections on NHS digital data projects and Data Sharing Agreements added
		Further considerations around using storage on local hard drives/solid state drives and portable devices added
		All audio recordings should only be on encrypted devices.
	Section 5	Extra information and links to University guidance on anonymisation added. Updated DSA templates added. Emphasis added to the signing of DSAs by an authorised signatory in Research Services
	Section 6	Updated to reference the latest guidance on reporting an incident. Also, added instruction to staff on reporting outside of normal working hours.
	Section 8	Requirement for data processing agreements to be signed by Research Services added.
9th August 2019	General	Following a review of how IT support is provided across the Faculty ScHARR IT support is now provided by the Faculty of MDH IT Team. A new ScHARR group for information governance and data security issues has been established, ScHARR DS. Therefore references to ScHARR IT has been changed to either Faculty IT or ScHARR DS accordingly.
	Section 2	A new subsection regarding hardware restrictions has been added.
	Section 3	Further clarification regarding the restriction of Google Drive added. Clarified the definition and use of audio recorders.
	Section 5	A link to Section 251, accessing confidential patient information without consent, has been added.

17th April 2020	Throughout	CiCs is now IT Services, web links updated
	Overview	Definition of risk bearing data updated to clarify that it includes pseudonymised
	Section 1	University data security training modules to be completed annually and policy enforcement clarified.
	Section 2	The detailed asset register applies to any study using the DSPT as the security assurance. Clarity added around hardware management (previously called restrictions) and device destruction section added.
	Section 3	High Performance Computing added Extra clarification around limitations of google drive added Updated to include any studies using DSPT as the security assurance on the asset register Additional guidance on data destruction added
	Section 4	Link to COVID-19 specific working from home policy added and removal of requirement for line manager written approval; reworded/restructured to clarify.
	Section 5	Information about privacy notices and opt outs added
	Section 6	Additional text has been added to the policy to ensure the IG Lead is aware of data specific requirements and notification details and discusses these with named liaison with ICO.
Oct 2020	Overview	Definition of risk-bearing updated slightly to personal, sensitive or confidential data; rather than and.
	Section 3	audio/video recording section updated to take into account extended remote working.
Jan 2021	Section 1	Cyber Safety training is now mandatory and the scope of Cyber Essentials has changed (it is now only mandatory for those staff whose research uses the DSPT as their data security assurance). The training section has been updated to reflect this.
May 2021	Section 4	advise regarding public Wi-Fi added
Jan 2022	Definitions	Data Safe Haven added
	Section 1	Updated to include potential use of Data Safe Haven for DSPT assured projects
	Section 2	Updated to bring it in line with current working practices around remote and hybrid working
	Section 3	Updated to add DSH, links to further processes and updates to CE+ registration process. Some updates to layout to make the flow more logical.
	Section 5	A note added about ensuring the DSA is clear regarding data to be shared.
	Section 7	Updates to links
Jun 2022	Section 1	Updated to make it very clear the training also applies to Honorary members of staff. Updated to indicate that CE+ registration is desirable but not mandatory;

		if not used compliance with the DSPT must be confirmed.
	Section 3	Updated to indicate that CE+ registration is desirable but not mandatory; if not used compliance with the DSPT must be confirmed.
	Section 7	Replaced link to approved destinations with UK list of adequacy decisions. Removed bullet regarding data transfers being permitted where they have given consent as this is a reference to the 1995 Data Protection Directive, which has been replaced by GDPR, and is no longer accurate
Jun 2023	Throughout	Where links are included within the policy these are not also included as footnotes. Ensured links throughout are up to date. Addition of references to new or updated processes added where relevant. Minor changes made to some wording to aid clarity.
	Definitions	Clarified that anonymising data is not as simple as removing direct identifiers. Additional definitions added to aid understanding.
	Section 1	Cyber Essentials Plus is no longer relevant
	Section 2	clarified information about personal devices, added a link to new equipment disposal and reallocation process. Simplified the section regarding the hardware inventory register.
	Section 3	Data Safe Haven is now Secure Data Service. Git has been added as an external services where the risks need to be considered. Reference to DPIAs made. CE+ no longer relevant. VM and SDS sections merged as both under the control of Central IT. Section on local storage removed, this is against policy. No longer including examples of data restrictions, DSAs and contracts should be referred to. X drive is preferred storage option, so order changed.
	Section 5	Research Services have asked us not to include the DSA templates in our policy
	Section 6	Included the Reporting a data breach guidance, emphasised the university procedures as these take precedence. Added failure to follow ScHARR IG policy or procedures as an example incident. Removed reference to incident management guidance made available by NHS Digital as this section is applicable regardless of data source
Apr 2024	Throughout	Replaced ScHARR with Division of Population Health, and School with Division, in accordance with the restructure. Removal of some bookmark links (replaced with a reference to the relevant section, as they don't work on the website.
May 2024	Throughout	Minor updates throughout to improve readability, update or remove redundant links, provide clarity etc
	Section 1	Updates to training section to reflect updates to systems within the university and to provide clarification.
	Section 3	Stanage has replaced ShARC References to Blackboard Collaborate have been removed, this is a teaching tool rather than research and the IG policy is primarily concerned with research data. Removed requirement to only record audio, this is an ethical rather than IG consideration.
	Section 5	Considerations around sharing of data without consent (unless section

		251 approved) has been removed.
	Section 6	Additional example incidents around sharing or saving of passwords have been added