NHS Improvement

Information and data handling policy

February 2019

collaboration trust respect innovation courage compassion

We support providers to give patients safe, high quality, compassionate care within local health systems that are financially sustainable.

Contents

Document control information

Document owner	Jeremy Marlow	Senior Information Risk Owner
Author	Catherine Abrams	Information Governance Manager
Reviewed by	Carol Mitchell	Head of Corporate Information Governance and Data Protection Officer
Approved by	Information Governance Group	Approvers of information governance policies and guidance

Version history

Version number	Version date	Revised by	Description of change
0.1	27 Aug 17	C Abrams	First draft
1.0	14 Sep 17	C Abrams	Reviewer/approver feedback incorporated
1.1	12 Dec 18	C Abrams	Policy review

1. Purpose

NHS Improvement holds personal data about our employees, suppliers and other bodies or people for business purposes and to provide its services. The lawful and proper handling of data by NHS Improvement is very important to the success of our business, helping us maintain the confidence of our service users and employees.

This policy sets out how we seek to protect personal data and ensure all staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) is consulted before any significant new data-processing activity is initiated to ensure that relevant compliance steps are taken.

2. Scope

This policy applies to all staff, including those on secondment, contracts or third parties. You must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to internet and email use. It applies to all processing of personal data in electronic form, including electronic mail and documents, or where it is held in manual files.

3. Key responsibilities

NHS Improvement's Data Protection Officer (see below) has overall responsibility for the day-to-day implementation of this policy.

3.1 The Accountable Officer

The Chief Executive has overall responsibility for ensuring that all NHS Improvement policies comply with legal, statutory and good practice guidance requirements.

3.2 The Caldicott Guardian

The Guardian is accountable for supporting the sharing of personal confidential data where it is appropriate to do so. They are registered on the publicly available National Register for Caldicott Guardians, are a member of the Executive Committee and attend the Information Governance Group.

3.3 Senior Information Risk Owner

The Senior Information Risk Owner is responsible for NHS Improvement's risks and provides a focus for the management of information risk at executive level; they are also chair of the Information Governance Group.

3.4 The Data Protection Officer

The Data Protection Officer (DPO) is empowered to act independently and should have the ability and resources required to perform the tasks specified in the General Data Protection Regulation (GDPR):

- provision of advice to the organisation on compliance obligations, and when a data protection impact assessment is required
- monitoring compliance with the GDPR and organisational policies
- co-operating and liaising with the Information Commissioner
- taking into account information risk when performing the above.

Further requirements of the role include:

- the DPO directly reports to the highest management level of the organisation
- there is timely involvement of the DPO in all data protection issues
- the DPO is supported by the necessary resources and is able to maintain expertise
- the DPO is not pressurised by the organisation on how to perform their tasks, and is protected from disciplinary action when carrying out those tasks
- where the DPO performs another role or roles, there is no conflict of interest.

3.5 IT and infrastructure manager responsibilities

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Check and scan security hardware and software regularly to ensure it is functioning properly.

- Research third-party services, such as cloud services, that NHS Improvement is considering using to store or process data.

3.6 Responsibilities of the individual

Through appropriate training and responsible management:

- observe all forms of guidance, codes of practice and procedures about the collection, processing or storage of data
- observe a duty of confidentiality and a responsibility to safeguard any data they access which is not in the public domain, regardless of whether the data is marked/classified
- sign the terms and conditions of employment which include specific data protection and confidentiality clauses
- ensure access to all information systems is password protected; passwords must not be disclosed to unauthorised persons (an authorised person will be an IT administrator, who may ask for a password to resolve an IT issue)
- ensure you do not log onto any system using someone else's password; this action is considered a serious breach of confidentiality and a disciplinary offence
- ensure that personal data NHS Improvement holds about you is accurate and updated as required, for example, if you move job role or address.

Additionally, staff should avoid:

- talking about official data in public places
- leaving any official data unattended
- leaving a laptop or computer terminal unlocked while not in use, where official data can be accessed.

4. Individuals' rights

One focus of GDPR is on individuals' rights, including:

- the right to be informed: our obligation to provide 'fair processing information', typically through a privacy notice
- the right of access: to ensure individuals are aware of and can verify the lawfulness of processing

- the right to rectification: for an individual to have personal data rectified if it is inaccurate or incomplete
- the right to erasure: also known as the ‘right to be forgotten’, to enable the deletion or removal of personal data
- the right to restrict processing: individuals have the right to ‘block’ or suppress processing
- the right to data portability: allows individuals to obtain and reuse their personal data for their own purposes across different services
- the right to object: to certain processing or direct marketing
- rights in relation to automated decision-making and profiling: which could impact on the individual without their knowledge.

5. Consent

Consent must be freely given, specific, informed and unambiguous. There must be a positive ‘opt-in’. Consent cannot be inferred from silence, pre-ticked boxes or inactivity.

6. Processing data

6.1 Fair and lawful processing

We must process personal data fairly and lawfully and in accordance with individuals’ rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening. The processing of all data must be:

- necessary to deliver our services
- in our legitimate interests and not unduly prejudice the individual’s privacy.

6.2 Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

6.3 Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose, unless the individual or organisation concerned has agreed to this or would otherwise reasonably expect this.

6.4 Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be securely disposed of when no longer needed.
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- The DPO must approve any cloud service used to store personal data.
- Servers containing personal data must be kept in a secure location.
- Data should be regularly backed up in line with NHS Improvement's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers containing sensitive data must be approved and protected by security software and firewalls.

6.5 Information asset register

Regular data audits to manage and mitigate risks will inform the information asset register. This contains information on what data is held by NHS Improvement, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

6.6 Data-sharing agreements

Any request to access personal data or data held by NHS Improvement belonging to a third party must be sent to IT.Support@improvement.nhs.uk and NHSI.ig@nhs.net. Most third-party organisations sharing data with NHS Improvement require a data-sharing agreement (DSA). A DSA sets out details of the data to be shared and agreed provisions relating to the handling of the data; how it will be accessed, shared, stored, used and disposed of.

Data shared under a DSA must only be used for the purposes specified in the DSA. Under no circumstances must any other person or group be granted access; the DSA can be amended to include additional people or a change in purpose as required.

All signed DSAs are retained securely by Information Governance for monitoring and review.

6.7 Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons the personal data was obtained, and should be determined in a manner consistent with the Records Management Code of Practice for Health and Social Care 2016.

All personal data should be deleted or securely destroyed once you have confirmed there is no need to retain it.

6.8 Transfer of data

If transfer of information is unavoidable, any papers, electronic storage or other approved devices containing such information must be transported in a secure way, and only the minimum amount of data required should be taken off premise. If the information is to be brought back on premise, this must be done as soon as it is no longer required off site. If the information is destroyed off premise, you must obtain a signed Certificate of Data Destruction and forward this to NHSI.ig@nhs.net.

Mobile devices or hard copy data must be kept on your person at all times when away from an office location or must be secured when not in use. Do not forward any personal data received under a DSA to a personal email account or store it on a privately-owned computer or device.

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations without the same protections in place as EU member states, to ensure the level of protection of individuals is not undermined. You must not transfer data outside the EU without consultation with NHSI.ig@nhs.net.

7. Privacy by design and default

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. It ensures data protection requirements are identified and addressed when designing new systems or processes. The responsible project or product owner will be responsible for conducting data protection impact assessments with support from the Information Governance team.

8. Privacy notice – transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. Each external-facing website should feature a privacy notice which should include:

- what information is being collected
- who is collecting it
- how it is collected
- how it will be used
- who it will be shared with
- identity and contact details of our data controller(s)
- details of transfers to third countries and safeguards
- retention periods.

9. Subject access requests

Under the GDPR, individuals have the right to obtain:

- confirmation that their data is being processed
- access to their personal data
- other supplementary information; this largely corresponds to the information that should be provided in a privacy notice.

We must provide a copy of information free of charge, unless the request is considered excessive. It must be provided without delay and at the latest, within one month of receipt. If you receive a subject access request, you should refer that request immediately to NHSI.foi@nhs.net.

10. Reporting a breach, near miss or cyber security incident

All staff have an obligation to report actual or potential data protection breaches or near misses to NHSI.ig@nhs.net, following the Incident Reporting and Management Procedure. Examples include:

- the loss of a mobile device containing sensitive information or data
- information or data being sent to an incorrect email recipient
- information or data being left on display, for example, left on a printer or copier
- accidental loss or deletion of information or
- unauthorised access to Official Sensitive information.

This allows us to investigate the failure and take remedial steps if necessary, maintain a register of compliance failures and notify the Information Commissioner's Office of any compliance failures that are material, either in their own right or as part of a pattern of failures.

11. Training and awareness: staff

All staff will be asked to familiarise themselves with this and other key policies as part of their induction. New joiners will be required to complete their mandatory information governance training before being given access to any systems or data, with all other staff required to complete their refresher training annually.

12. Training and awareness: staff, contractors and third parties

All staff, contractors or third parties employed by NHS Improvement must observe this policy. Information Governance will monitor regularly to ensure adherence.

Corporate IT and infrastructure, together with Information Governance, may from time to time perform surveillance on the IT estate and examine logs or run queries to understand its usage and highlight any potential confidentiality breaches. See the Internet, Email and Telecommunications Policy for more detail.

13. Consequence of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk and may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything within this policy, do not hesitate to contact NHSI.ig@nhs.net.

Contact us:

NHS Improvement
Wellington House
133-155 Waterloo Road
London
SE1 8UG

0300 123 2257
enquiries@improvement.nhs.uk
improvement.nhs.uk

@NHSImprovement

This publication can be made available in a number of other formats on request.

 Publication code: CG 11/19