Data Breach Policy and Procedure

NHS Property Services

Document Name, Version Number & Approval Date	Title: Data Breach Policy and Procedure Version Number:2.1 Approval Date: December 2021

Policy Owner	Department: Information Governance

Supporting Procedures & Additional Information	Data Protection Act 2018 General Data Protection Regulation Information Governance Policy Data Protection Impact Assessment Policy Data subject rights policy Access to CCTV Policy Corporate Records Management Policy Acceptable Use Policy Whistleblowing Policy Code of Conduct or other People Team related policies/procedures www.ico.org.uk

NOTE: This policy should be reviewed annually and may be amended or replaced at any time.

DOCUMENT HISTORY

Version	Issue Date	Author(s)	Summary of Changes
V2.1		Head of Information Governance Senior Information Governance Lead	Contains new appendices detailing breach reports and remediation tracking.

CONTENTS

1. PURPOSE

1.1. NHS Property Services (NHSPS) has a duty to protect and safeguard personal data. Whilst we take all appropriate measures to protect personal data (based on risk and cost), we acknowledge and understand that no organisation can guarantee 100% security.

1.2. Our responsibilities for handling data and reporting data breaches are set out in the Data Protection Act 2018 and the General Data Protection Regulation.

1.3. This policy will set out a clear procedure to best mitigate any incidents where personal data has been compromised. In addition, where such compromised data includes 'personal data', this Policy also sets out the additional requirements that need to be met to ensure that our obligations in relation to the protection of personal data are also met.

1.4. Failure to comply with this policy or data protection legislation may result in serious repercussions for both the organisation and the individual concerned.

1.5. Organisations may face significant fines of up to 4% of global turnover or €20,000,000 (whichever is higher).

1.6. Individuals may face penalties such as criminal proceedings in cases of negligence, fraud or deliberate misuse.

1.7. For further information on data breaches or information related legislation, please visit the GDPR intranet page GDPR (sharepoint.com) or contact the Information Governance team by emailing dpo@property.nhs.uk.

2. SCOPE

2.1. This framework applies to all colleagues within NHSPS, including agency staff, independent contractors, honorary contracts, volunteers, trainees, and students on work experience placements.

3. RESPONSIBILITIES

All Colleagues

3.1. NHSPS expects all colleagues to operate in accordance with this policy and within the scope of their role.

3.2. You should report any actual, suspected, threatened or potential data breach immediately to your line manager, the Information Governance team and the Data Protection Officer (DPO).

All managers

3.3. All managers are responsible for ensuring all members of their team act in compliance with this policy.

3.4. Line Managers should take all reasonable steps to contain the breach and mitigate the impact and work with the DPO to investigate the suspected data breach.

DPO

3.5. The DPO is responsible for overseeing this policy and developing data-related policies and guidelines.

3.6. The DPO has the responsibility to make final decision on data breaches and incidents and whether to report to the ICO.

3.7. The DPO will report all data breaches to the SIRO and the Executive Committee.

3.8. The DPO will work with the Legal team if any claims in relation to a data breach are received.

Information Governance Team

3.9. The Information Governance Team is responsible for investigating potential data breaches and maintaining a list of all data breaches.

3.10. The IG team will inform the Senior Information Risk Officer and DPO when Data breaches have been received.

SIRO

3.11. The SIRO should be informed of data breaches as they occur and be a recipient of the Data Breach report form to assess the level of risk exposure of the data breach.

3.12. The SIRO should assess the whether the lessons' learned/recommendations within the report are sufficient for mitigating future risks.

Cyber Security Team

3.13. The Cyber Security team will be informed if data breaches arise from a cyber security incident.

3.14. The team and will work with the Information Governance team to ensure:

- The current incident is dealt with immediately.
- Sufficient controls are introduced to mitigate the recurrence of the incident.

Legal Team

3.15. The Legal Team will liaise with NHS Resolution if there is a claim in relation to a data breach.

4. Data Breach Definition

4.1. A data breach is where we have lost control of personal data that we should be holding and protecting. The GDPR defines a personal data breach as:

"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. (article 4(12))".

4.2. The DPO has **48 hours** from discovery of the data breach to determine whether the breach is likely to affect the rights or freedoms of any living individual.

4.3. If a breach has been determined, the DPO should inform the SIRO and report to the ICO within **72 hours** of discovery.

5. Data Breach Types

5.1. Whilst data breaches may present themselves in many ways, data breaches can fall within one or more of the following categories:

- **Confidentiality Breach** – Unauthorised or accidental disclosure of, or access to personal data
- **Availability Breach** – Unauthorised or accidental loss of access to, destruction of personal data
- **Integrity Breach** – Unauthorised or accidental alteration of personal data.

	ICO Breach Categorisation	Type of Breach (Article 29 Working Party)
A	Data sent by email to incorrect recipient	Confidentiality
B	Data posted or faxed to incorrect recipient	Confidentiality
C	Failure to redact data	Confidentiality
D	Information uploaded to webpage	Confidentiality
E	Cyber Security misconfiguration (e.g. inadvertent publishing of data on website	Confidentiality
F	Failure to use bcc when sending email	Confidentiality
G	Cyber Security misconfiguration (e.g. inadvertent publishing of data on website; default passwords	Confidentiality
H	Cyber incident (phishing)	Confidentiality
I	Insecure webpage (including hacking)	Confidentiality
J	Cyber incident (key logging software)	Confidentiality
K	Loss or theft of paperwork	Availability
L	Loss or theft of unencrypted data	Availability
M	Loss/theft of only copy of encrypted data	Availability
N	Data left in insecure location	Availability
O	Cyber incident (other - DDOS etc.)	Availability
P	Cyber incident (exfiltration)	Availability
Q	Cryptographic flaws (e.g. failure to use HTTPS; weak encryption)	Availability

R	Insecure disposal of paperwork	Availability
S	Insecure disposal of hardware	Availability
T	Other principle 7 failure	Integrity
U	Cyber incident	Integrity

6. Reporting a Data Breach

6.1. NHSPS must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

6.2. Examples of where the breach may have a significant effect includes:

- potential or actual discrimination,
- potential or actual financial loss,
- potential or actual loss of confidentiality,
- risk to physical safety or reputation,
- exposure to identity theft (for example through the release of non-public identifiers such as passport details),
- the exposure of the private aspect of a person's life becoming known by others.

6.3. If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

7. Assessing high risk to individuals' rights and freedoms?

7.1. Both the severity of the potential or actual impact on individuals because of a breach and the likelihood of this occurring should be assessed. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher.

7.2. The Article 29 Working Party says that "This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached".

7.3. To help assess the severity of a breach, the ICO has selected examples taken from various breaches reported to the ICO. These also include helpful advice about next steps to take or things to think about, and can be found at Personal data breach examples | ICO.

8. Data Breach Procedure

Discovering a breach

8.1. If you discover a data breach, you must immediately inform your line manager, the Information Governance team and the Data Protection Officer (DPO).

8.2. The line manager and Information Governance team should take all reasonable steps to contain the breach and mitigate the impact. This includes but is not limited to:

- recovering the data,
- requesting and confirming that data has been deleted by third parties,
- re-issuing information as appropriate, and
- identify whether the data included special data.

8.3. The DPO should issue advice and guidance as required.

Reporting a breach

8.4. You and/or your line manager should complete the data breach report form as far as possible (**Appendix 1**) and send to dpo@property.nhs.uk **within 24 hours**. This should be submitted as a document by email. If special data is thought to be included in the data loss, the DPO should be informed immediately.

8.5. The Information Governance team should acknowledge receipt of the breach and approach the line manager to discuss where appropriate. If the data breach report form has been completed, the Information Governance team will CC in the relevant director.

8.6. The Information Governance team will update the data breach register and inform the Senior Information Risk Owner (SIRO), Cyber Security, People team, and Counter Fraud as appropriate.

8.7. Having dealt with containing the breach, the Information Governance team will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out below), and include:

- The type of data is involved and how sensitive it is.
- The volume of data affected.
- Who is affected by the breach (i.e. the categories and number of people involved).
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise.
- Whether there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation).
- What has happened to the data.
- What could the data tell a third party about the data subject.
- What are the likely consequences of the personal data breach on NHSPS; and
- Any other wider consequences which may be applicable.

8.8. The Data breach report form should be fully completed and signed off by the Information Governance team and shared with the SIRO and any Stakeholder deemed appropriate.

Notifying Data Subjects

8.9. The DPO should decide **within 48 hours** of discovery of the data breach as to whether the breach is likely to affect the rights or freedoms of any living individual. See **Appendix 2** for examples of when to notify Data Subjects.

Notifying the ICO

8.10. If the breach is likely to affect the rights or freedoms of any living individual, the DPO should decide if to refer to the ICO. If yes, the DPO should report to the ICO without delay, and **within 72 hours** of becoming aware of the breach. The Chief Executive should also be notified.

8.11. If the DPO is unsure of whether to report a breach, the assumption should be to report it. Further guidance can be found at Data breach reporting | ICO, and examples are found in **Appendix 2.**

8.12. If no, the DPO to recommend case closure and the Senior Information Governance Officer should close the case on the tracker.

8.13. If the 72-hour limit is breached, or is expected to breach, the DPO should seek advice from appropriate sources such as legal professionals or the ICO.

9. Preventing Future Breaches

9.1. Once the data breach has been dealt with, the Information Governance team will document the lessons learned / recommendations required to improve processes and awareness with the aim of preventing further breaches in the Data Breach form. We will:

- Establish what security measures were in place when the breach occurred.
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again.
- Consider whether there is adequate awareness of security issues across the organisation and look to fill any gaps through training or tailored advice.
- Consider whether it is necessary to conduct a privacy or data protection impact assessment.
- Consider whether further audits or data protection steps need to be taken.
- Update the data breach register.
- Update the DPO/SIRO/Caldicott Guardian forum and ExCo following the investigation.

9.2. A separate Data Breach recommendation tracker will also be maintained to ensure all mitigations are actioned timely (**see Appendix 3**). This will be reported to the SIRO/DPO/Caldicott Guardian meeting, and to the relevant Executive Director where actions for improvement sit.

10. Legal Claim

10.1. If a claim is pursued via legal proceedings, this will be received by the Legal team.

10.2. Claims received by Legal should be provided to the DPO, to enable an investigation to be performed to determine the strength of the claim and the risk of it being upheld.

10.3. NHS Resolution should be informed of any claims which may incur a compensation payment.

11. TRAINING

11.1. The Data Protection Officer has responsibility for awareness-raising and training on all matters related to Information Governance, including data breaches. The training provided will be reviewed on a regular basis by the Information Governance team to ensure it remains relevant.

All-employee Mandatory Training

11.2. The following mandatory training modules are hosted on the learning Zone and must be completed by all colleagues annually:

- Data Protection.
- Confidentiality.

11.3. These modules will support the understanding of what may constitute a data breach and what should be done in the event that one occurs.

Focussed Training

11.4. The Information Governance team will identify areas of the business where additional training is required, should a number of data breaches occur in that area.

11.5. Additional training can also be requested for teams or individuals requiring further information or to enable roles to be performed appropriately.

12. MONITORING

12.1. Compliance will be monitored by the Data Protection Officer.

12.2. Data breaches will be logged and reported to the DPO/SIRO/Caldicott Guardian monthly meeting and to the ExCo.

12.3. Audits may be carried out by the Data Protection Officer and their team to determine compliance of data protection legislation.

12.4. In cases of non-compliance, disciplinary measures may be taken in accordance with People policies and the code of conduct. Decisions about disciplinary measures will be determined by the relevant Director.

13. REVIEW

13.1. This policy is to be reviewed every two years or upon any significant change to data protection legislation. This will be led by the Information Governance team and the data protection officer.

APPENDIX 1 – DATA BREACH REPORTING FORM

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

If we identify a personal data breach, we must consider whether this poses a risk to people, and the likelihood and severity of the risk to people's rights and freedoms following the breach. Following this assessment, if it's likely there will be a risk then we must notify the ICO; if it's unlikely then we don't have to report.

We do not need to report every breach to the ICO.

Data Breach Details	
Data Breach Number	*IG Team to complete*
Date and Time of Breach	*When and what time did the data breach happen?*
Breach identified by	*Name, job title and Department of person who has identified the breach.*
Breach reported to and when	*Who has this been reported to and how?*
Details of Breach	***What happened?*** *Please provide a* ***brief*** *overview of the breach - no more than 50 words.*
What personal data has been lost/accessed?	*Provide details of data that has been lost/ accessed/deleted etc, e.g. names, addresses, emails, online identifiers). NB: Financial data is* ***not*** *personal data* *Does this include any special category data?* *Racial or ethnicity, Health, Genetic data, Criminal data, Biometric data, Political opinions, religious beliefs, Trade Union membership*
Data Breach Investigation	
Evidence reviewed	*Include documents and personnel spoken to*
Investigation Findings	*Provide a detailed overview of findings including:* • *Why did the data breach occur?* • *Number of records lost?* • *Number of data subjects affected?* • *Has the data been recovered?* • *Does the data subject know?* • *Has a complaint been received?* • *Has something similar happened before?* • *What steps you have taken to mitigate the breach* • *Any other relevant information to the case.*
Data Breach Outcome **(to be completed by Information Governance team)**	

Investigation Outcome	*What is the opinion of the severity of the breach?* *What is the likelihood of harm occurring to the data subject (Not occurred, Not likely, Likely, Highly Likely, Occurred)?* *What impact could this have/has this has on the data subject (No impact, Minor, Adverse, Serious, Catastrophic)?*
Reported to ICO	*Yes/No*
Recommendations / Lessons Learned	*What will be done to stop this happening again?*
Report written by	
Date report signed off	

APPENDIX 2 - EXAMPLES OF WHEN TO REPORT

The following non-exhaustive examples will assist in determining whether we need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendation
NHSPS has stored a backup of an archive of personal data encrypted on a USB key. **The key is stolen during a break-in.**	No	No	As long as the data are encrypted with a state-of-the-art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
NHSPS maintains an online service. As a result of a cyber-attack on that service, personal data of individuals are exfiltrated.	Yes, report to the ICO if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high	
A brief power outage lasting several minutes at a NHSPS call centre meaning customers are unable to call the NHSPS and access their records.	No	No	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
NHSPS suffers a ransomware attack which results in all	Yes, report to the ICO, if there are likely consequences to	Yes, report to individuals, depending on the nature of the personal data	If there was a backup available and data could be restored in good time, this would not need to be reported to the ICO or to individuals as there would

data being encrypted. **No back-ups are available, and the data cannot be restored.** **On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.**	individuals as this is a loss of availability	affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	have been no permanent loss of availability or confidentiality. However, if the ICO became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
NHSPS operates an online marketplace. The marketplace suffers a cyber-attack and usernames,	Yes, report to the ICO.	Yes, as could lead to high risk.	NHSPS should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. NHSPS should also consider

passwords and purchase history are published online by the attacker.			any other notification obligations, e.g. under the NIS Directive as a digital service provider
A website hosting company acting as a data processor identifies an error in the code which controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay. Assuming that the website hosting company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.	If there is likely no high risk to the individuals, they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive as a digital service provider). If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have occurred, but it is likely to be recordable or be a matter of non-compliance under Article 32.
Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to ICO	Yes, report to individuals depending on the scope and type of personal data involved and the severity of	

		possible consequences.	
A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the ICO may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

APPENDIX 3 – DATA BREACH RECOMMENDATION TRACKER

This will be used to track the implementation of recommendations made within a Data Breach investigation.

Data Breach Number	Recommendation	Recommendation Owner (person and team)	Management Comment	Deadline for Implementing	Status Update