Information Governance:

Data Breach Policy

|  |
| --- |
| **Policy** |
| **Applies to:** | All staff & stakeholders |
| **Date Issued:** | 1st March 2018 |
| **Status** | Ratified |
| **Version** | 4 |
| **Date for Review** | March 2022 |

Information Governance:

Data Breach Policy

[POLICY HEADER](#_Policy_Header)

[REVISION HISTORY](#_Revision_History)

[DEFINITIONS](#_Definitions)

[DATA BREACH POLICY](#_Data_Breach_Policy)

[1: INTRODUCTION](#_1:_Introduction)

[2: PURPOSE AND SCOPE](#_2:_Purpose_and)

[3: TYPES OF BREACH](#_3:_Types_of)

[4: EXAMPLES OF BREACHES](#_4:_Examples_of)

[5: REPORTING AN INCIDENT](#_5:_Reporting_an)

[6: CONTAINMENT AND RECOVERY](#_6:_Containment_and)

[7: INVESTIGATION AND RISK ASSESSMENT](#_7:_Investigation_and)

[8: NOTIFICATION](#_8:_Notification)

[9: EVALUATION AND RESPONSE](#_9:_Evaluation_and)

[10: POLICY REVIEW](#_10:_Policy_Review)

[11: DUTIES](#_11:_Duties)

[12: IMPLEMENTATION](#_12:_IMPLEMENTATION)

[13: TRAINING](#_13:_TRAINING)

[14: TARGET AUDIENCE](#_14:_TARGET_AUDIENCE)

[15: MONITORING COMPLIANCE](#_15:_MONITORING_COMPLIANCE)

[16: CONSULTATION](#_16:_CONSULTATION)

[17: RELEVANT ORGANISATION POLICIES](#_17:_RELEVANT_ORGANISATION)

[18: EQUALITY IMPACT ASSESSMENT](#_18:_EQUALITY_IMPACT)

[19: LEGISLATION COMPLIANCE](#_19:_LEGISLATION_COMPLIANCE)

[20: REVIEW DATE](#_20:_REVIEW_DATE)

[21: CHAMPION AND EXPERT WRITER](#_21:_CHAMPION_AND)

[22: REFERENCES / SOURCE DOCUMENTS](#_22:_REFERENCES_/)

# POLICY HEADER

|  |  |
| --- | --- |
| **Applies to** | All employees & stakeholders |
| **Date Issued** |  |
| **Status** | Provisional |
| **Version** | 1.0 |
| **Date for Review** |  |

# REVISION HISTORY

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Summary of Changes** |
| 1.0 | 2018-03-01 | Initial version |

# DEFINITIONS

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Organisation | R & F EMERSON LLP (Sussex Community Dermatology Service, Hove Skin Clinic, Brighton Laser Clinic, Worthing Skin Clinic) |
| Personally Identifiable Information (PII) | Information which can uniquely identify an individual. For the purposes of this policy *information* and *data* are synonymous |
| Sensitive Information | A special category of sensitive personal data e.g., racial origins or mental and physical health |
| General Data Protection Regulation | A regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA) |

# DATA BREACH POLICY

## 1: INTRODUCTION

1.1: The Organisation holds, processes and shares personally identifiable information, an asset valuable both to the individuals it refers to and to the Organisation. As the Organisation’s activity focuses on healthcare services much of this data is also of a sensitive nature.

1.2: Every care must be taken to protect personal data.

1.3: Compromise of information confidentiality, integrity, or availability may result in: harm to individual(s), reputational damage, a detrimental effect on service provision, legislative non-compliance and / or financial costs.

1.4: This document sets out the framework that staff should follow in the event of discovering, or otherwise being made aware of, a data breach concerning data processed or held by the organisation.

## 2: PURPOSE AND SCOPE

2.1: The Organisation is obliged under the General Data Protection Regulation to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2: This policy sets out the procedures to be followed to ensure a consistent and effective approach is in place for managing data breach incidents within the Organisation.

2.3: This policy relates to all personally identifiable information – including special category sensitive data - held by the Organisation, regardless of format.

2.4: This policy applies to all staff and students at the Organisation. This includes: temporary, casual or agency staff, contractors, consultants, suppliers and data processors working for, or on behalf of the Organisation.

2.5: The objective of the policy is to contain any breaches, to minimise any risk associated with the breach and to consider any remediate actions required to secure the personal data and minimise the chances of future breaches.

## 3: TYPES OF BREACH

3.1: For the purposes of this policy, data security breaches include **both** confirmed and suspected incidents.

3.2: A breach in the context of this policy means 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.

3.3: Breaches are broadly categorised as confidentiality, availability or integrity although a breach may cover all categories.

3.4: **Confidentiality breaches** involve the unauthorised disclosure of, or access to personal data.

3.5: **Availability breaches** involve the unauthorised or accidental loss of access to, or destruction of, personal data.

3.5: **Integrity breaches** involve the unauthorised or accidental alteration of personal data.

## 4: EXAMPLES OF BREACHES

4.1: Breaches include, but are not limited to, the following:

* Loss or theft of confidential or sensitive data or unencrypted equipment on which such data is stored (e.g., loss of laptop, USB stick, a patient’s medical record).
* Equipment theft or failure.
* System failure
* Unauthorised use of, access to, or modification of data or information systems.
* Attempts (regardless of success) to gain access to data or information systems.
* Unauthorised disclosure of personally identifiable or sensitive data.
* Website defacement.
* Hacking attack against the network.
* Social hacking attack – a ‘blagging’ offence where access is gained by deceiving employees.
* Fire, flood or other unforeseen disaster having a detrimental effect on the availability of data.
* Human error.

## 5: REPORTING AN INCIDENT

5.1: Any individual who accesses, uses or manages the Organisation’s data is responsible for reporting a data breach and any related information security incidents immediately to the Data Protection Officer and to the Information Security Officer.

5.2: If a breach occurs or is discovered outside of normal working hours, it must be reported as soon as is practicable.

5.3: The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the data, and how many individuals are involved. A **Data Breach Report Form** should be completed as part of the reporting process. These can be found on the Organisation’s intranet.

## 6: CONTAINMENT AND RECOVERY

6.1: The Data Protection Officer will first determine if the breach is still occurring. If so, the appropriate steps will be taken to immediately minimise the effect of the breach.

6.2: An initial assessment will be made by the Data Protection Officer in liaison with the relevant employees to establish the severity of the breach and who will take the lead in investigating the breach further as the Lead Investigation Officer (this will depend on the nature of the breach – in some cases this will be the Data Protection Officer).

6.3: The Lead Investigation Officer will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

6.4: The Lead Investigation Officer will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

6.5: Advice from the experts within the Organisation may be sought in resolving the incident promptly, including the Senior Information Risk Officer.

6.6: The Lead Investigation Officer, in liaison with any relevant employee(s) will determine the suitable course of action to ensure a resolution to the incident.

## 7: INVESTIGATION AND RISK ASSESSMENT

7.1: An investigation will be undertaken by the Lead Investigation Officer immediately and when possible, within 24 hours of the breach being discovered / reported.

7.2: The Lead Investigation Officer will investigate the breach and assess the risks associated with it. For example, the potential adverse consequences for individuals, how serious or substantial the risks are and how likely they are to occur.

7.3: The investigation will need to consider the following:

* The type of data involved;
* Its sensitivity;
* The protections that are in place (e.g., encryption and password policies);
* What has happened to the data (e.g., has it been lost or stolen);
* Where the data could be put to any illegal or inappropriate use;
* Data subject(s) affected by the breach, the number of individuals involved and the potential effects on those data subject(s);
* Whether there are wider consequences to the breach;

## 8: NOTIFICATION

8.1: The Lead Investigation Officer and the Data Protection Officer, in consultation with the Senior Information Risk Owner and any relevant employees will establish whether the Information Commissioners Office (ICO) will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where practicable.

8.2: Every incident will need to be assessed for particulars; however, the following will need to be considered:

* Whether the breach is likely to result in a high risk of adversely affecting individual’s rights and freedoms under the General Data Protection Regulation;
* Whether notification would assist the individual(s) affected (e.g., could they act on the information themselves to mitigate risks?);
* Whether notification would help prevent the unauthorised or unlawful use of personal data;
* Whether there are any legal or contractual notification requirements (e.g., to a particular *Care Commissioning Group*);
* The dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.

8.3: Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual’s rights and freedoms will be informed without delay. Notifications will include a description of how and when the breach occurred and the date involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the Organisation for further information or to ask questions on what has occurred.

8.4: The Lead Information Officer and / or the Data Protection Officer must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

8.5: The Lead Information Officer and / or the Data Protection Officer will consider whether Marketing Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

8.6: A record will be kept of any personal data breach, regardless of whether notification was required.

8.7: If notification is deemed as the necessary response, the Data Protection Officer in liaison with the Senior Information Risk owner will use the online portal provided at <https://www.dsptoolkit.nhs.uk/Incidents> to report the breach. Any resulting outputs from the tool must be kept separately (i.e., downloaded and filed with the Information Governance Team).

## 9: EVALUATION AND RESPONSE

9.1: Once the initial incident is contained, the Data Protection Officer will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

9.2: Existing controls will be reviewed to determine their adequacy, and whether any corrective action(s) should be taken to minimise the risk of similar incidents occurring.

9.3: The review will consider:

* Where and how personally identifiable information is held and how it is stored;
* Where the biggest risks lie including identifying potential weak points within existing security measures;
* Whether methods of transmission are secure; sharing the minimum amount of data necessary;
* Staff awareness, including any remedial training required;

9.4: If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Senior Information Risk Owner and actioned as appropriate.

## 10: POLICY REVIEW

10.1: This policy will be updated as a necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

## 11: DUTIES

11.1: All NHS records are public records under the terms of the Public Records Act 1958 S.3(1)-

(2). The Act sets out the broad responsibilities of everyone who works with such records and

provides for guidance and supervision by the Keeper of Public Records.

11.2: All NHS bodies have a statutory duty to make arrangements for the safe-keeping and

eventual disposal of their records.

11.3: The Chief Executive, as accountable officer, is responsible for the management of the

organisation, and for ensuring appropriate mechanisms are in place to support service

delivery and continuity. Records management is key to this as it will ensure appropriate,

accurate information is available as required.

11.4: The Caldicott Guardian is responsible for ensuring that patients’ interests are maintained

regarding holding, obtaining, recording, using and sharing their information.

11.5: The Organisation’s Senior Information Risk Officer (SIRO) has board level accountability for all risks related to data and information security.

11.6: An Information Asset Owner (IAO) will be identified for each information asset

(system). These will have overall responsibility for managing the risks to the assets.

11.7: Information Asset Administrators (IAA) will be identified for information assets

(systems). IAOs may delegate responsibility for managing the information risks to the

IAAs, however, overall responsibility remains with the IAO.

11.8: It is the duty of Managers at all levels to ensure that their staff are aware of and adhere to this policy. They are also responsible and accountable for ensuring their staff are updated in regard to any changes in this policy. All line managers and supervisors have a duty to

ensure that their staff, whether administrative or clinical, are adequately trained and apply the appropriate guidelines and professional standards.

11.9: Clinical directors, directorate managers and all in managerial or supervisory roles have the responsibility for developing and encouraging good data handling practice within their designated areas.

11.10: All Organisation staff, whether clinical or administrative, who create, receive and use data have data protection responsibilities. In particular all staff must ensure that they process data appropriately in the Organisation and manage data in keeping with this policy and with any guidance subsequently produced. It is the responsibility of all staff to adhere to the policy’s principles and procedures to help maintain the availability, effectiveness, security and confidentiality of information.

11.11: Everyone working for, or with the NHS, who records, handles, stores or otherwise comes across information has a personal common law duty of confidentiality. The Data Protection Act 1998 and subsequent General Data Protection Regulation places statutory restrictions on the use of personal information, including health information. Accordingly, all staff members are directly responsible and accountable for keeping accurate and complete records of their activities.

## 12: IMPLEMENTATION

12.1 All organisation staff will be made aware of their responsibilities for data management through generic and specific training programmes. It is the responsibility of the Information Asset Owner to ensure that individual training needs are identified and met for existing and new staff. All new staff must receive training on information management in general and on the management of departmental records as part of their induction.

## 13: TRAINING

13.1: All staff should be aware of this policy, the data management procedures and the Information Governance procedures. Staff should know how to access copies of these from the Intranet.

13.2: The Organisation will put in place training and guidance for all staff involved in the creation, maintenance and ongoing management of health and corporate data.

## 14: TARGET AUDIENCE

14.1: All employees.

## 15: MONITORING COMPLIANCE

15.1: The implementation and effectiveness of this policy will be assessed by the Information Governance Steering Group. This will facilitate the reporting mechanism ensuring issues and concerns are reported through to the appropriate chairs of Organisation groups, Committees and the Organisation Board.

15.2: The Organisation will regularly audit its records management practices for compliance with this policy framework.

15.3: All staff are responsible for monitoring their compliance with the principles detailed in this policy; departmental managers and supervisors should also monitor compliance on a regular basis.

15.4: This policy will be continually monitored and will be subject to a regular review. The review will be carried out by the Data Protection Officer working with other staff as appropriate.

## 16: CONSULTATION

16.1: Within the Organisation via the Information Governance Steering Committee and Board of Directors

## 17: RELEVANT ORGANISATION POLICIES

* Information Security Incident Management & Investigation Procedures Policy
* Network and Application Security Policy
* Records Management Policy
* Clinical Records Management
* Freedom of Information Act
* Information Governance Policy
* Information Risk Management Policy
* Staff Training Policy

## 18: EQUALITY IMPACT ASSESSMENT

18.1: This policy has been assessed using the Equality Impact Assessment Screening Tool. The assessment concluded that the policy would have no adverse impact on, or result in the positive discrimination of, any of the diverse groups detailed.

## 19: LEGISLATION COMPLIANCE

19.1: The Organisation has obligations to ensure adherence to the following legislation and policy:

* The Public Records Act 1958
* The Data Protection Act 1998
* Freedom of Information Act 2000
* Records Management NHS Code of Practice (Part 1 and 2)

## 20: REVIEW DATE

20.1: This policy will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are to be introduced).

## 21: CHAMPION AND EXPERT WRITER

21.1: The Champion of this policy is Christopher Emerson, Information Governance Lead.

## 22: REFERENCES / SOURCE DOCUMENTS

22.1: This policy has been developed with reference to the following documents:

* NHS Code of Practice: Records Management
* NHS Code of Practice: Confidentiality
* The Caldicott Committee Report on the Review of Patient - Identifiable Information.
* HSG (96) 18 The Protection and Use of Patient Information
* HSC 1998/153 Using Electronic Records in Hospitals - Legal Requirements and Good Practice
* HSC 1998/168 Information for Health
* Delivering 21st Century IT for the NHS
* The Health Archives Group’s booklet: Hospital Patient Case records - A Guide to their Retention and Disposal. Advice about selection processes of records disposal.
* Audit Commission, Setting the Record Straight, 1995
* Standards on Record Keeping within CNST, and Information Governance Standards
* Lord Chancellor's Code of Practice on the Management of records issued under Section 46 of The Freedom of Information Act 2000.
* General Medical Council. Confidentiality: Guidance for doctors, 2009
* DSP IR Guidance: <https://www.dsptoolkit.nhs.uk/Help/Attachment/101>