Trust-wide Document

NHS
Great Western Hospitals
NHS Foundation Trust

Data Security & Protection Incident Reporting Procedure

Document No	IG - 00004	**Version No**	2.0
Approved by	Policy Governance Group	**Date Approved**	14.11.18
Ratified by	Information Governance Steering Group	**Date Ratified**	02.11.18
Date implemented (made live for use)	13.12.18	**Next Review Date**	13.12.21

Status	LIVE
Target Audience- who does the document apply to and who should be using it.	All employees directly employed by the Trust whether permanent, part-time or temporary (including fixed-term contract). It applies equally to all others working for the Trust, including private-sector, voluntary-sector, bank, agency, locum, and secondees. For simplicity, they are referred to as 'employees' throughout this policy
Special Cases	None
Accountable Director	Director of Finance / Senior Information Risk Owner (SIRO)
Author/originator – Any Comments on this document should be addressed to the author	Senior Information Governance Officer
Division and Department	Finance / Corporate
Implementation Lead	Information Governance Manager / Data Protection Officer
If developed in partnership with another agency ratification details of the relevant agency	N/A
Regulatory Position	• General Data Protection Regulation (Ref 1) • Data Protection Act 2018 (Ref 2) • The Security of Network and Information Systems Directive (NIS Directive) [Ref 3]
Review period. This document will be fully reviewed every three years in accordance with the Trust's agreed process for reviewing Trust -wide documents. Changes in practice, to statutory requirements, revised professional or clinical standards and/or local/national directives are to be made as and when the change is identified.	

Contents

1 Introduction & Purpose

The General Data Protection Regulation (GDPR) [Ref 1], as implemented by the Data Protection Act 2018 (DPA 2018) [Ref 2], came into UK law on 25 May 2018. It introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority, which in the UK is the Information Commissioner's Office (ICO). The Security of Network and Information Systems Directive ("NIS Directive") [Ref 3] also required reporting of relevant incidents to the Department of Health and Social Care (DHSC) as the competent authority from 10 May 2018.

Organisations must keep a record of any personal data breaches, regardless of whether it is required to notify them to external organisations (see Section 2.5.3 of this procedural document). Therefore, this document provides a clear and simple process for employees to follow to report data security and protection incidents, and a clear and simple mechanism for investigating such incidents and resolving them satisfactorily.

This procedure has been developed to assist Trust employees in identifying data security and protection incidents, suspected information security weaknesses or near misses, security threats to services or systems and how to report such incidents through the appropriate channels.

If this process is followed correctly, it will assist the Trust to maintain the integrity, confidentiality and availability of the information that it holds, processes and shares. It will also enable the Trust to mitigate risks, to develop and improve good practice and to put in place robust measures for preventing recurrence of data security and protection incidents.

Please note that concerns relating to physical security (including acts of terrorism), fraud etc. are to be raised under the appropriate process or policy (e.g. the Security Policy [Ref 4], or the Fraud and Corruption Policy [Ref 5]).

1.1 Glossary/Definitions

The following terms and acronyms are used within the document:

CQC	Care Quality Commission
DHSC	Department of Health and Social Care
Disclosable	Information which may be disclosed, for example, in relation to a subject access request
DPA	Data Protection Act (2018)
DSPT	Data Security & Protection Toolkit
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
IG	Information Governance
IT	Information Technology
IGSG	Information Governance Steering Group
NHS Digital	The national information and technology partner to the health and social care system (formerly known as the Health & Social Care Information Centre [HSCIC])
NIS Directive	Security of Network and Information Systems Directive
NPSA	National Patient Safety Agency
Personal Data	Any information relating to an identified or identifiable living individual
UK	United Kingdom
SIRO	Senior Information Risk Owner
STEIS	Strategic Executive Information System
EIA	Equality Impact Assesment

2 Main Document Requirements

2.1 Data Security and Protection Incidents

A data security and protection incident is 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. It can also include incidents that prevent access to, destruction of, or modification to the Trust's data.

The GDPR (Ref 1) affirms that any data breach that creates a risk to the rights and freedoms of an individual is a personal data breach and therefore could be notifiable (see Section 2.5.3 of this document). This overrides previous concepts that a data breach is only reportable when data falls into the wrong hands.

There are three types of breaches:

- Confidentiality – unauthorised or accidental disclosure of or access to personal data;
- Availability - unauthorised access to or destruction of personal data, or data is unavailable or cannot be accessed;
- Integrity - unauthorised or accidental alteration of personal data.

Examples of data security and protection incidents are given at Appendix B of this document. The latter two breach types (availability and integrity) include cyber threats and threats to business continuity and further information about this is also provided in Appendix B of this document.

2.2 Reporting Data Security and Protection Incidents

Employees may become aware of actual or potential data security and protection incidents through a variety of means. For example, another employee, through observing someone in their working practice, or there may be a system malfunction caused by an information technology (IT) security breach.

It is important that immediate steps are taken to ensure that the risks to information security and/or patient or employee confidentiality are minimised. For example, if an employee finds a document containing staff or patient personal data in a public area, they should make a note of where they found it and take it with them for safe-keeping, thus ensuring that no-one else will be able to read it.

In all instances it is the employee's responsibility to ensure that such incidents are reported through the appropriate channels (see Sections 2.2.1 to 2.2.4 of this document) and that any reports produced are directed to the most appropriate officers for investigation and resolution.

Incident reports help the Information Governance (IG) team to identify any occurrences which are the same or similar and to ensure that where areas of vulnerability are identified, actions are taken to mitigate risks to the Trust's data. When reporting an incident, it is important to provide as much detail as possible to enable the team to understand and respond appropriately to the incident. Therefore it is good practice to include a description of any activities which led up to the incident, information about circumstances prevailing at the time, how the incident came about and how it was detected.

The message to all employees is "if in doubt – report it". If, after investigation, the incident is scored low, or classed as a near miss this still helps to mitigate the risk of a serious breach occurring as appropriate controls or procedures can be put in place to prevent this.

There are several ways in which a data security and protection incident may be reported:

2.2.1 Reporting via the Trust's Incident Reporting System

The process described in the Trust's Incident Management Policy (Ref 6) can be used for reporting data security and protection incidents. If the cause of the incident is recorded in the incident reporting and management system as a "Breach of Confidentiality", an incident notification email will be sent to the IG team, who may, if deemed necessary, carry out an independent investigation into the incident.

Depending on the nature of the incident, the IG Team may also receive notification of incidents where the cause has been identified as relating to personal data/records, such as patient mis-identification, records mix-up/misfiled etc.

The incident report form must be completed as soon as the incident is discovered, or no later than the end of the shift on the day that it is discovered. Incident forms are a disclosable record, and as such, must be professional, factual and not exaggerated. Incident forms may be seen by other individuals and organisations external to the Trust, such as the National Patient Safety Agency (NPSA), the Care Quality Commission (CQC), solicitors and patients, therefore the description must not contain personal details such as patient or staff names.

If the incident is assessed as being notifiable to external bodies, the IG Team will follow the process described in Section 2.5.3 of this document. As notification must take place within 72 hours of the Trust becoming aware of the incident, it is important that incidents are reported promptly.

2.2.2 Reporting via the IT Service Desk

The majority of incidents which involve the accessibility or availability of information held on the Trust's IT systems will be reported via the IT Service Desk. If an employee becomes aware of anything untoward, they must report this to the IT Service Desk without delay. They may be contacted on 01793 60(5858), or by email: gwh.itservicedesk@nhs.net. The IT Service Desk will take the user's details and a record/summary description of the issue and will assign the call to the appropriate team in the IT Department to investigate. The Information Governance (IG) Team will be notified of the incident if a risk to information security is reported.

2.2.3 Reporting via the Information Governance Team

The IG team can investigate any actual or suspected data security and protection incident. The team can also provide confidential advice to anyone who is unsure about reporting an incident or who has a concern about anything related to data protection and security. The team can be contacted on 01793 60(5675) or email: gwh.info.gov@nhs.net.

If the IG Team considers the incident to be reportable, they will ask the employee to complete an electronic incident report, as described in Section 2.2.1 of this document.

2.2.4 Reporting a Concern

If an employee has a concern about a suspected or actual breach of confidentiality, they have a right and a duty to raise this with the Trust. The Trust in turn has a duty to ensure that employees can feel safe to raise a concern and for conversations to take place as part of everyday practice, without fear of blame or reprisal. Employees are encouraged to report any concerns they have to their Line Manager in the first instance who will initiate appropriate investigations.

In some instances an employee may not feel comfortable in reporting their concern(s) to their Line Manager. Concerns may be raised in confidence, and therefore can be raised without the employee's

identity having to be disclosed without their consent. Concerns raised in this way will be dealt with in accordance with the Trust's Freedom to Speak up Policy (Ref 7).

2.3 Recording and Classifying Data Security and Protection Incidents

It is essential that data security and protection incidents are accurately recorded and classified in order that they can be reported and/or notified appropriately. The IG Team will log all reported incidents into a database set up for that purpose and will produce reports that can be provided for the Information Governance Steering Group (IGSG) to review and if required for external reporting.

2.3.1 Grading Personal Data Breaches

Any reported incident must be graded according to the severity (impact) and the likelihood that citizen's rights have been affected (harm). The incident must be graded according to the impact on the individual or groups of individuals concerned and not on the organisation (the Trust).

As the breach assessment grid provided in the 'Guide to the Notification of Data Security and Protection Incidents' provided by NHS Digital [Ref 8] varies from the standard risk matrix used in the Trust, the IG team will review all reported incidents to determine their grading. This will then determine whether the incident has to be notified to any external bodies (see Section 2.5.3 of this document).

2.4 Incident Management Process

This procedure will conform as much as possible to the process for investigating all adverse incidents described in the Trust's Incident Management Policy (Ref 6). This will ensure that the management of data security and protection incidents which are notifiable to external bodies (see Section 2.5.3 of this document) is consistent with overarching Trust policy, and that the policy will take precedence should a conflict arise with this procedure. The process is the same, although the external organisations that require notification will vary from those listed in the policy document.

2.4.1 Incident Investigation

Upon being notified of an incident, a member of the IG Team will review the incident, and using the 'Guide to the Notification of Data Security and Protection Incidents' provided by NHS Digital (Ref 8), will decide whether the incident requires further investigation, whether it requires notification, whether it needs to be reported externally (for example in the Trust's annual report), or whether it can be logged and closed.

As notification must take place within 72 hours of the Trust becoming aware of the incident, it is important that incidents are reported promptly and that the IG Team review the incident report on receipt.

If an investigation is required, the IG Team may decide to conduct this, or they may pass the report to the relevant manager to conduct the investigation. The investigation can take different forms depending on the nature of the incident and the grading given to it (see Section 2.3.1 of this document), and employees may obtain further guidance on how to conduct the investigation from the Incident Management Policy (Ref 6).

It is most important that the investigation includes collecting evidence relevant to the incident, recording facts and that follow-up action is taken. Evidence may be in the form of a written statement, a letter from a patient or an audit trail from an electronic system, for example.

2.4.2 Follow-up Action

Follow-up action can take several forms depending on the nature of the incident, whether it has happened before (a repeat of the same or a very similar incident), or whether it is likely to recur. It may include:

- Referral to the Human Resources Department or to the Trust's Local Counter Fraud Specialist;
- Issuing communications to a department or to the Trust as a whole as a reminder;
- Recommending additional training and development to be undertaken;
- If caused by an IT system, a recommendation to purchase additional software or equipment such as a robust anti-virus solution.

The GDPR (Ref 1) requires any personal data breach that is likely to result in a high risk to the rights and freedoms of individual(s) to be communicated with those affected. The communication must contain:

- A description of the nature of the breach;
- The name and contact details of the Data Protection Officer for the Trust;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken or proposed to be taken by the Trust to address the breach, and where appropriate, to mitigate any potential adverse effect.

If an employee is unsure whether this is required, or needs guidance on how to word the appropriate communication, they should contact the IG Team in the first instance who will be able to provide advice and assistance.

There are some circumstances where it may not be necessary to inform the individuals concerned, and these are:

- When security measures have been implemented which were applied to the personal data affected by the breach, for example, the loss of data held on removable media which has been encrypted;
- Subsequent measures have been taken to ensure that the high risk to the rights and freedoms of individual(s) is no longer likely to materialise;
- It would involve disproportionate effort, e.g. large numbers of individuals were or may have been affected. (However, it may still be possible to communicate this, for example via a notice on the website, or a press notice); or
- If the communication relating to a breach would cause the data subject disproportionate distress or harm.

2.5 Reporting and Notification of Incidents

2.5.1 Internal Reporting

The Trust's IG Steering Group (IGSG) reviews a summary report each month on the number of reported incidents, the grades they have been assigned and which category they fall into. They also review an annual summary report giving total statistics for the financial year. They will also be asked to review and confirm the grading given to any incident which would involve external reporting or notification (see Sections 2.5.2 and 2.5.3 of this document). If the IG Team wants to highlight anything to the IGSG which is deemed unusual, is happening on a regular basis, or may require follow-up by Senior Managers, they will do this at the next IGSG meeting.

2.5.2 External Reporting

The 'Guide to the Notification of Data Security and Protection Incidents' provided by NHS Digital states that incidents notifiable to the ICO and/or the DHSC should be included in the Trust's Annual Report. These incidents need to be detailed individually in the report in the format shown below. All reported incidents relating to the period in question should be reported.

Date of incident (month)	Nature of incident	Number affected	How individuals were informed	Lesson learned

2.5.3 Notification

The Data Security and Protection Incident Reporting Tool is an online system imbedded within the Data Security and Protection Toolkit (DSPT) [Ref 9]. This tool has been agreed by NHS Digital and the ICO for reporting personal data security breaches. The IG Team has access to this tool and will use it to record details of any incident which is considered to be serious enough to warrant external notification.

The tool asks a series of questions related to the incident and there is a chance to review the answers before the incident is reported. The report does not have to be completed in one go, but it does have to be notified within 72 hours.

Dependant on the responses to the questions contained in the reporting tool, the information provided will be sent to the ICO, the DHSC and the National Cyber Security Centre (Ref 10). If it is considered a serious incident which needs notification, it will also have to be reported on the NHS serious incident management system, Strategic Executive Information System (STEIS) or its successor, as well as the DSPT. The local STEIS number can be added to the DSPT reporting tool. In some cases, the responses to the questions will confirm that the incident is not serious enough to warrant notification and it will then state 'Not required to report'.

The ICO's guidance on notifying data security breaches (Ref 11) states that the overriding consideration in deciding whether to report a breach is the potential for detriment to data subjects. Where there is little risk of significant detriment, there is no need to notify. Examples of this are given in Appendix B of this document.

There are a limited number of circumstances where, even when an organisation is aware of a breach of personal data, there may be containment actions that will remove the need for notification to the ICO but may still need to be recorded as a near miss as it may still constitute a reportable occurrence under the NIS directive (Ref 3).

Under the following circumstances notification may <u>not</u> be necessary:

- encryption – where the personal data is protected by means of encryption;
- 'trusted' partner* - where the personal data is recovered from a trusted partner organisation; or
- cancel the effect of a breach - where the controller can null the effect of any personal data breach.

* A trusted partner would be the wrong department of the same organisation a commonly used supplier or an organisation with which the Trust has an on-going relationship. They can be "trusted" not to read or access the data sent in error and to comply with the instructions to delete or return it.

3 Monitoring Compliance and Effectiveness of Implementation

The arrangements for monitoring compliance are outlined in the table below: -

Measurable policy objectives	**Monitoring / audit method**	**Monitoring responsibility** (individual / group /committee)	**Frequency of monitoring**	**Reporting arrangements** (committee / group to which monitoring results are presented)	**What action will be taken if gaps are identified?**
To ensure that all reported data security and protection incidents are reviewed, logged and investigated, and that a systematic approach is adopted in accordance with this procedure.	All reported incidents are reviewed by the IG Team and areas of non-compliance with this procedure are addressed.	IG Team	As required	IG Steering Group	The IG Team will develop an action plan and present it to the IG Steering Group for approval. This will be monitored at the monthly meetings and closed once recommendations have been implemented.
	All incidents are reported to the IGSG in summary form, and any that are deemed to be notifiable are reported in detail.	IG Team	As required	IG Steering Group	

4 Duties and Responsibilities of Individuals and Groups

4.1 Chief Executive

The Chief Executive is ultimately responsible for the implementation of this document.

4.2 Ward Managers, Matrons and Managers for Non Clinical Services

All Ward Managers, Matrons and Managers for Non Clinical Services must ensure that employees within their area are aware of this document; able to implement the document and that any superseded documents are destroyed.

4.3 Employees

Employees are responsible for:

- Understanding the principles of confidentiality, integrity and availability, and recognising what constitutes a personal data breach;
- Reporting all data security and protection incidents via the electronic reporting system in a timely manner;
- Where the employee is involved in or is witness to an incident, the Trust requires them to take immediate steps to ensure that the risks to information security and/or patient or employee confidentiality are minimised;
- Ensuring any training required is attended and kept up to date;
- Ensuring any competencies required are maintained;
- Co-operating with any investigation;
- Co-operating with the development and implementation of policies as part of their normal duties and responsibilities.

4.4 Line Managers

All line managers must ensure that they review the initial risk assessment assigned to the incident and oversee any further immediate actions which need to be taken. This includes upward notification and the timely completion of any investigation documentation.

Line managers are responsible for ensuring that feedback is provided to all their employees on the results of investigations and that any resultant action taken to prevent recurrence. Line managers have responsibility for ensuring that all employees who report to them have adequate information, instruction, training and supervision in the management of data security and protection incidents.

4.5 The Information Governance Team

The IG Team is responsible for ensuring compliance with processes defined within this document, ensuring that all reported incidents are reviewed, logged and investigated as appropriate, making recommendations to managers and the IG Steering Group for processes to be put in place to minimise the risk of recurrence and the provision of monthly, six-monthly and ad hoc reports on data security and protection incidents to the IG Steering Group.

4.6 Document Author and Document Implementation Lead

The document Author and the document Implementation Lead are responsible for identifying the need for a change in this document as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and resubmitting the document for approval and republication if changes are required.

4.7 The Information Governance Steering Group

As described in Section 2.5.1 of this document, the IG Steering Group has responsibility for monitoring and reviewing data security and protection incidents and related Trust policies and for overseeing the reporting process and confirming the grading assigned to incidents is accurate. They must also ensure that incidents are managed effectively and that appropriate steps are taken to minimise the risk of recurrence. This includes reviewing incident detail and trends using data and reports which are prepared each month by the IG Team for this purpose.

5 Further Reading, Consultation and Glossary

5.1 References, Further Reading and Links to Other Policies

The following is a list of other policies, procedural documents or guidance documents (internal or external) which employees should refer to for further details:

Ref. No.	Document Title	Document Location
1	General Data Protection Regulation 2016	https://gdpr-info.eu
2	Data Protection Act 2018	http://www.legislation.gov.uk
3	The Security of Network and Information Systems Directive (NIS Directive)	https://www.ncsc.gov.uk
4	Security Policy	T:\Trust-wide Documents
5	Fraud and Corruption Policy	T:\Trust-wide Documents
6	Trust Incident Management Policy	T:\Trust-wide Documents
7	Freedom to Speak Up Policy	T:\Trust-wide Documents
8	Guide to the Notification of Data Security and Protection Incidents published by NHS Digital	https://www.dsptoolkit.nhs.uk
9	Data Security and Protection Toolkit	https://www.dsptoolkit.nhs.uk
10	National Cyber Security Centre	https://www.ncsc.gov.uk
11	ICO Guidance on notifying data security breaches	https://ico.org.uk

5.2 Consultation Process

The following is a list of consultees in formulating this document and the date that they approved the document:

Job Title / Department.	Date Consultee Agreed Document Contents
IG Support Officer, Finance	1st October 2018
IG Manager, Finance	1st October 2018
Deputy Director of Finance (Contracts and Informatics)	2nd November 2018
Quality Lead, Clinical Risk	2nd November 2018
Health Records Manager	2nd November 2018
Deputy Chief Nurse	2nd November 2018
Clinical Risk Advisor, Clinical Risk	7th November 2018

6 Equality Impact Assessment

An Equality Impact Assessment (EIA) has been completed for this document and can be found at Appendix A.

Appendix A - STAGE 1: Initial Screening For Equality Impact Assessment

At this stage, the following questions need to be considered:			
1	What is the name of the policy, strategy or project? Data Security & Protection Incident Reporting Procedure		
2.	Briefly describe the aim of the policy, strategy, and project. What needs or duty is it designed to meet? Describes the process to be followed to report and manage data security and protection incidents. The Trust has a duty under data protection regulations and laws to report these types of incident.		
3.	Is there any evidence or reason to believe that the policy, strategy or project could have an adverse or negative impact on any of the nine protected characteristics (as per Appendix A)?		**No**
4.	Is there evidence or other reason to believe that anyone with one or more of the nine protected characteristics have different needs and experiences that this policy is likely to assist i.e. there might be a *relative* adverse effect on other groups?		**No**
5.	Has prior consultation taken place with organisations or groups of persons with one or more of the nine protected characteristics of which has indicated a pre-existing problem which this policy, strategy, service redesign or project is likely to address?		**No**

Signed by the manager undertaking the assessment	Mark Arnold
Date completed	14/11/2018
Job Title	IG Manager

On completion of Stage 1 required if you have answered YES to one or more of questions 3, 4 and 5 above you need to complete a STAGE 2 - Full Equality Impact Assessment

Appendix A – Equality Impact Assessment

Equality Impact Assessment

Are we Treating Everyone Equally?

Define the document. What is the document about? What outcomes are expected?

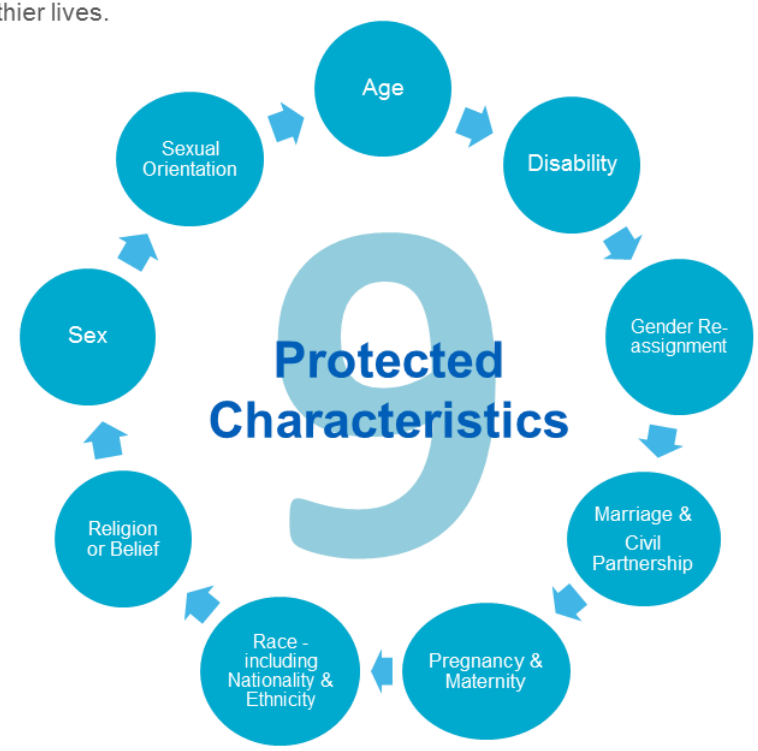
Consider if your document/proposal affects any persons (Patients, Employees, Carers, Visitors, Volunteers and Members) with protected characteristics? Back up your considerations by local or national data, service information, audits, complaints and compliments, Friends & Family Test results, Staff Survey, etc.

If an adverse impact is identified what can be done to change this? Are there any barriers? Focus on outcomes and improvements. Plan and create actions that will mitigate against any identified inequalities.

If the document upon assessment is identified as having a positive impact, how can this be shared to maximise the benefits universally?

Our Vision

Working together with our partners in health and social care, we will deliver accessible, personalised and integrated services for local people whether at home, in the community or in hospital empowering people to lead independent and healthier lives.



Trust Equality and Diversity Objectives

Better health outcomes for all	Improved patient access & experience	Empowered engaged & included staff	Inclusive leadership at all levels

Appendix B – Examples of Data Security and Protection Incidents

Example	Breach Type	Notes (to help assess the grading)
A medical record of a child is sent to the wrong department in the same hospital.	Confidentiality	The department receiving that record would be considered "trusted".
A single ward handover sheet identifying patients and their medical conditions is found in the hospital car park.	Confidentiality	During the time that the sheet was in the car park a breach may have occurred.
A loss of one patient's case notes which is likely to lead to problems in treating the patient.	Availability	This loss has caused harm to the patient in that a problem with treating them has arisen due to the loss of their case notes.
A cyber incident (see below) similar to the 2017 WannaCry incident where it cannot be detected whether any data has been lost, but it affects the availability of clinical services.	Availability	There is a risk to patients that harm may occur if clinical appointments have to be cancelled.
It is discovered that a website has been hacked and the information that is provides has been defaced.	Integrity	This is unlikely to result in harm to individuals as the website does not contain personal data.
Notes from a patient outpatient appointment are recorded in a different patient's record.	Integrity	Potentially there could be a clinical consequence of this breach if treatment is arranged for the wrong patient.

Although the examples given relate to patient data, they can equally apply to data relating to other individuals that the Trust holds, such as employees.

Cyber Threats and Business Continuity

The Security of Networks and Information Systems Regulations 2018 (NIS Regulations) [Ref 3] seek to ensure that essential services, including healthcare, have adequate data and cyber security measures in place to deal with the increasing volume of cyber threats. They require operators of essential services to report any network and information systems incident which has a 'significant impact' on the continuity of the essential service that they provide to the relevant 'competent authority'.

Any data, network or information system incident affecting the delivery of health or social care services is likely to be notifiable. The same process, as described in this document, is to be used. Further detailed guidance is available in the Guide to the Notification of Data Security and Protection Incidents published by NHS Digital (Ref 8).