AUDIOLOGICAL SCIENCE
NHS AND PRIVATE AUDIOLOGY SERVICES

Audiological Science Ltd.
5 Hoop Lane
London NW11 8JR
Tel – 0208 059 9645
Email – audiologicalscience.barnet@nhs.net

Data Protection & Breach Policy

Purpose and objectives

To identify potential data security breach risks, specify safeguards, and state information handling in the event of a breach.

To meet the seventh data protection principle of the Information Commissioner's Office (ICO), which is:

- "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

Scope

All data relating to Audiological Science Ltd, its patients and service users and staff, as employees of the organisation held within the organisation or with any of its professional associates, however stored.

Introduction

Information is a vital asset, both in terms of the clinical management of individual patients/service users and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

This document outlines our policy and commitment to dealing with Data Protection and further to detail processes for any Data Breach received about any of the services provided by Audiological Science Ltd. The document is also intended to serve as a guidefor all operational staff working at Audiological Science Ltd. ("the Organisation")

Audiological Science Ltd. are committed to learning from complaints/feedback and apply those lessons to best practice.

Aims

This policy outlines procedures and responsibilities within Audiological Science Ltd. for data protection, including the management of Data Breaches, in the event of an information security incident.

The terms information security incident and suspected incidents are very broad. They include, but are not limited to, incidents that relate to the loss, disclosure, denial of access to, destruction or modification of the Organisation's information, or information systems.

An information security incident can be defined as any event that has resulted or could result in:

- The disclosure of confidential information to an unauthorised individual
- The integrity of a system or data being put at risk
- The availability of the system or information being put at risk

An adverse impact can be defined for example as:

- Threat to personal safety or privacy
- Legal obligation or penalty
- Financial loss
- Disruption of Organisation business
- An embarrassment to the Organisation

Examples of security incidents:

- Using another user's login id/swipe card
- Unauthorised disclosure of information
- Leaving confidential / sensitive files out
- Theft or loss of IT equipment
- Theft or loss of computer media, i.e. floppy disc or memory stick
- Accessing a person's record inappropriately e.g. viewing your own health record or family members, neighbours, friends etc.,
- Writing passwords down and not locking them away
- Identifying that a fax or email has been sent to the wrong recipient
- Sending/receiving a sensitive email to/from "all staff" by mistake
- Giving out or overhearing personally identifiable information over the telephone
- Positioning of pc screens where information could be viewed by the public
- Software malfunction
- Inadequate disposal of confidential material

Diligent employees should question procedures, protocols and events that they consider could cause damage, harm, distress, break of compliance or bring the Trust's name into disrepute

Relevant CQC Fundamental Standard/ H&SC Act Regulation (2014)
Regulation 15: "Premises and Equipment".
Regulation 17: "Good governance"

Responsibilities

All staff working at Audiological Science Ltd. are required to able to act in accordance with this policy in relation to all information received and stored by the Organization as personal data information about patients and service users. All staff have a responsibility to be aware of the policy, be aware of where to access the policy and follow the policy.

The Compliance Manager and Clinic Manager are responsible for logging all breaches and complaints regarding this policy inthe Audiological Science Logbook.

The Compliance Manager is responsible to ensure the policy is up to date, staff are trained on thepolicy and the training is logged.The Clinic Manager, Compliance Manager or Managing Director are responsible for communicationwith user associated with the suspected or real breach of information security.

The Compliance Manager and Managing Director are responsible for completing an audit every month on the data breaches incurred or suspected and creating an action log where required.

Learnings

All qualifying incidents should be logged in to the Audiological Science Compliance logbook. AudiologicalScience Ltd. are committed to learn from the suspected or real incidents to work towards improving the service we provide.

An audit will be completed once a month on all potential data breaches experienced by Audiological Science Ltd. Theaudit will be completed by the Compliance Manager and Managing Director.

The purpose of this audit is to ensure we:

- Identify trends within the service model.
- Highlight system or human failures.
- Ensure compliance log is being completed.
- Ensure incidents are being logged correctly and escalated appropriately.

The outcome report and action log findings will be presented to all staff during monthly staff meeting where every incident will be highlighted. This will include monthly incident numbers, patterns/trends and how we can learn and change our service to improve the quality of our care. In such instances there may be a change required in the clinical or non-clinical operations of the serviceand this will be reflected in the respective policies. The outcome report information may be used to share findings with commissioners of services.

In some cases, following on from an investigation, there may be immediate changes required to theservice provision and this information will be sent out via secured email to all staff. This will be included in the monthly outcome report and highlighted again in the monthly meetings.

Audiological Science Ltd. are committed to providing ongoing training to staff. The Audit outcome report and action log will be used to identify areas where training may be required. Training will be provided during monthly staff meetings and in some instances external online or classroom coursesmay be offered.

Effectiveness Criteria

It is vital that all incidents are logged and recorded for Audiological Science Ltd. to analyse the effectiveness of our Data Protection policy. The compliance log must be completed when reported to the Compliance Manager or ClinicManager. Notes must be clear, in plain English and in the service user's file for all actions and interactions.

The Data Protection Policy

Audiological Science Ltd., as an organisation which processes personal data, must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

Procedure

If breach has occurred, there are four important elements to any breach management plan:

- Containment and Recovery
- Assessment of ongoing risk
- Notification of breach
- Evaluation and response

This will then be followed by actions to repair the breach and set in place alternative business structures.

1. Containment

Data security breaches will require not just an initial response to investigate and contain the situation but also a Recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers. Consider the following:

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.
- Establish whether there is anything you can do to contain any losses and limit the damage the breach can cause. As well as the physical Recovery of equipment, this could involve the use of backup media to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, inform the police and the Information Commissioners Office (ICO).

2. Assessing the Risks

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged, but its files were backed up and can be retrieved, albeit at some cost to the business. While these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of an employee database, the data on which may be used to commit identity fraud. Before deciding on what steps are necessary, further to immediate containment, assess the risks which may be associated with the breach. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

The following points are also likely to be helpful in making this assessment:

- What type of data is involved?
- How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details).
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks.
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

3. Notification of Breaches

This means Informing people and organisations that you work with that the organisation has experienced a data security breach and can be an important element in your breach management strategy. However, informing people about a breach is not an end in itself.

- Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.
- From May 2018 all organisations (service providers) have a requirement to notify the

Information Commissioner (ICO), and in some cases individuals themselves, of personal data security breaches.

- For more information about the specific breach notification requirements for service providers- see ICO website: https://ico.org.uk/. Their general guidance is outlined below:

  - "Answering the following questions will assist other types of organisations in deciding whether to notify:
    - Are there any legal or contractual requirements? Service providers have an obligation to notify the Commissioner in certain circumstances. Health and Social Care providers will have a legal responsibility to notify their Regulator of breaches, and may have a contractual obligation to notify commissioners of services, such as Social Services or NHS.
    - Can notification help you meet your security obligations with regard to the seventh data protection principle? This is "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."
    - Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?
    - If a large number of people are affected, or there are very serious consequences, you should inform the ICO. There is normally a 72-hour deadline for doing this.
    - Consider how notification can be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.
    - Have you considered the dangers of 'over notifying'. Not every incident will warrant notification and notifying a whole customer base of an issue affecting only one customer may well cause disproportionate enquiries and work.

  - You also need to consider who to notify, what you are going to tell them and how you are going to communicate the message. This will depend to a large extent on the nature of the breach but the following points may be relevant to your decision:
    - Make sure you notify the appropriate regulatory body. A sector specific regulator may require you to notify them of any type of breach but the ICO should only be notified when the breach involves personal data.
    - There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation.
    - Your notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to respond to the risks posed by the breach.
    - When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them.
    - Provide a way in which they can contact you for further information or to ask you questions about what has occurred – this could be a helpline number or a web page, for example.

- When notifying the ICO you should also include details of the security measures in place such as encryption and, where appropriate, details of the security procedures you had in place at the time the breach occurred. You should also inform the ICO if the media are aware of the breach so that we can manage any increase in enquiries from the public. When informing the media, it is useful to inform them whether you have contacted the ICO and what action is being taken. ICO will not normally tell the media or other third parties about a breach notified to us, but we may advise you to do so.

- The ICO has produced guidance for organisations on the information we expect to receive as part of a breach notification and on what organisations can expect from us on receipt of their notification.
  - This guidance is available on the ICO website: https://ico.org.uk/
  - You might also need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions."

4. Evaluation and Response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of your response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if your response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and outline responsibility in the light of experience.

It may be found that existing procedures could lead to another breach and therefore it will be important to identify where improvements can be made.

The following points will be of assistance:

- Make sure you know what personal data is held and where and how it is stored. Dealing with a data security breach is much easier if you know which data are involved. Your notification with the Information Commissioner will be a useful starting point.
- Establish where the biggest risks lie. For example, how much sensitive personal data do you hold? Do you store data across the business or is it concentrated in one location?
- Risks will arise when sharing with or disclosing to others. You should make sure not only that the method of transmission is secure but also that you only share or disclose the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced.
- Identify weak points in your existing security measures such as the use of portable storage devices or access to public networks.
- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice.
- Consider whether you need to establish a group of technical and nontechnical staff who discuss 'what if' scenarios – this would highlight risks and weaknesses as well as giving staff at different levels the opportunity to suggest solutions.

- If you have completed the Business Continuity Plan for dealing with serious incidents, consider implementing a similar plan for data security breaches, or incorporating security breaches into the overall Business Continuity Plan. Breach of data security could in some circumstances be serious enough to endanger the business.

Other information

- Additional guidance is also available if you need further information on data security breaches: See Notification of data security breaches to the Information Commissioner's Office
- General advice: Department for Business Innovation and Skills

Following Up – After a breach of data privacy

Incidents should be used in training sessions about security and confidentiality as using 'real life events' relevant to an organisation can always be related to by staff, a lot better than in imaginary events. This will give the attendees and example of what could occur, how to respond to such event and how to avoid them in the future.

Appendix One

ICO data breach reporting form

Security Breach Notification Form

This form is for data controllers to report a breach of security to the ICO. It should take about five minutes to complete.

Before completing this form, you should read the following guidance: Notification of Data Security Breaches to the Information Commissioner's Office.

Please provide as much information as possible. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant information, e.g. incident reports.

Sending this Form

Send your completed form to casework@ico.gsi.gov.uk, with 'Security breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms sent by email.

What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

- A case reference number and;
- An explanation of what to expect during our investigation of the incident.

If you need any help in completing this form, please contact our helpline on:

0303 123 1113 or 01625 545745 (operates 9am and 5pm Monday to Friday).

1	What is the name of your organisation (the data controller)?	
2	Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)	
3	Have you notified as a data controller? If so, please provide your registration number. Search the online Data Protection Public Register.	
4	Have you reported any previous incidents to the ICO? If so, please provide brief details and reference numbers, where known.	
5	When did this incident occur?	
6	Please briefly describe the incident.	
7	Has any personal data been placed at risk? If so, please give us an outline of what this data consists of.	
8	Approximately how many data subjects have been affected?	
9	Have you informed the data subjects that this incident has occurred?	
10	Has there been any media coverage of the incident?	
11	Have you taken any action to minimise/mitigate the effect on the data subjects involved? If so, please provide brief details.	
12	Are you carrying out an investigation into the incident - If so, when will you complete it and what format will it take?	
13	Have you informed any other regulatory body of the matter? If so, please provide their details and an outline of their response.	
14	What action have you taken to prevent similar incidents in the future?	
15	Is there any other information you feel would be helpful to the ICO's assessment of this incident?	

Security Breach Notification Form

Appendix Two

The legal obligations around data privacy – GDPR Articles

Article 33 "Notification of a personal data breach to the supervisory authority"

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;
   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article

Article 34 – “Communication of a personal data breach to the data subject"

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
   (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
   (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
   (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Appendix Three

Assessing the Severity of the Incident Guide (IG SIRI)

Although the primary factors for assessing the severity level are the numbers of individual data subjects affected, the potential for media interest, and the potential for reputational damage, other factors may indicate that a higher rating is warranted, for example the potential for litigation or significant distress or damage to the data subject(s) and other personal data breaches of the Data Protection Act. As more information becomes available, the IG SIRI level should be re-assessed.

Where the numbers of individuals that are potentially impacted by an incident are unknown, a sensible view of the likely worst case should inform the assessment of the SIRI level. When more accurate information is determined the level should be revised as quickly as possible.

Please note: Conversely, when lost data is protected e.g. by appropriate encryption, so that no individual's data can be accessed, then there is no data breach (though there may be clinical safety implications that require the incident to be reported down a different route). When the data is protected but risk of individuals being identified remains an incident and should be reported. The sensitivity factors will reflect that the risk is low.

All IG SIRIs entered onto the IG Toolkit Incident Reporting Tool, confirmed as severity level 2, will trigger an automated notification email to the Department of Health, Health and Social Care Information Centre and the Information Commissioner's Office, in the first instance and to other regulators as appropriate, reducing the burden on the organisation to do so.

The IG Incident reporting tool works on the following basis when calculating the severity of an incident:

There are 2 factors which influence the severity of an IG SIRI – Scale & Sensitivity.

Scale Factors

Whilst any IG SIRI is a potentially a very serious matter, the number of individuals that might potentially suffer distress, harm or other detriment is clearly an important factor. The scale (noted under step 1 below) provides the base categorisation level of an incident, which will be modified by a range of sensitivity factors.
Sensitivity Factors

Following stakeholder feedback, the Sensitivity factors have been revised and are shown on the following page. Sensitivity in this context may cover a wide range of different considerations and each incident may have a range of characteristics, some of which may raise the categorisation of an incident and some of which may lower it. The same incident may have characteristics that do both, potentially cancelling each other out. For the purpose of IG SIRI investigations sensitivity factors may be:

Low – reduces the base categorisation
High – increases the base categorisation

Categorising SIRIs

The IG SIRI category is determined by the context, scale and sensitivity. Every incident can be categorised as level:

1. Level 0 or 1 confirmed IG SIRI but no need to report to ICO, DH and other central bodies/regulators.

2. Level 2 confirmed IG SIRI that must be reported to ICO, DH and other central bodies/regulators.

A further category of IG SIRI is also possible and should be used in incident closure where it is determined that it was a near miss or the incident is found to have been mistakenly reported:

0. Near miss/non-event
Where an IG SIRI has found not to have occurred or severity is reduced due to fortunate events which were not part of pre-planned controls this should be recorded as a "near miss" to enable lessons learned activities to take place and appropriate recording of the event.

The following process should be followed to categorise an IG SIRI

Step 1: Establish the scale of the incident. If this is not known it will be necessary to estimate the maximum potential scale point.

Baseline Scale (existing)	
0	Information about less than 11 individuals
1	Information about 11-50 individuals
1	Information about 51-100 individuals
2	Information about 101-300 individuals
2	Information about 301 – 500 individuals
2	Information about 501 – 1,000 individuals
3	Information about 1,001 – 5,000 individuals
3	Information about 5,001 – 10,000 individuals
3	Information about 10,001 – 100,000 individuals
3	Information about 100,001 + individuals

Step 2: Identify which sensitivity characteristics may apply and the baseline scale point will adjust accordingly.

Sensitivity Factors (SF) modify baseline scale

Low:	For each of the following factors reduce the baseline score by 1
	(A) No sensitive personal data (as defined by the Data Protection Act 1998) at risk nor data to which a duty of confidence is owed

-1 for each	(B) Information readily accessible or already in the public domain or would be made available under access to information legislation e.g. Freedom of Information Act 2000
	(C) Information unlikely to identify individual(s)

High:	For each of the following factors increase the baseline score by 1
+1 for each	(D) Detailed information at risk e.g. clinical/care case notes, social care notes
	(E) High risk confidential information
	(F) One or more previous incidents of a similar type in the past 12 months
	(G) Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information
	(H) Likely to attract media interest and/or a complaint has been made directly to the ICO by a member of the public, another organisation or an individual
	(I) Individuals affected are likely to suffer substantial damage or distress, including significant embarrassment or detriment
	(J) Individuals affected are likely to have been placed at risk of or incurred physical harm or a clinical untoward incident

The Incident Reporting Tool will not allow you to select sensitivity factors which would not be relevant based on initial selections. See below for settings and key for A to J sensitivity factors noted above.

When user selects this:	The following sensitivity factors are excluded:
A	D, E
B	D, E, I, J
C	I,J
D	A, B
E	A, B

F	Nothing excluded
G	Nothing excluded
H	Nothing excluded
I	B, C
J	B, C

Step 3: Where adjusted scale indicates that the incident is level 2, the incident should be reported to the ICO within the reporting timescales noted in this guidance. There is a 'notify later' option within the IG Incident Reporting Tool which can be used to save the incident for a short period to allow you to seek authorisation from local Senior Management or Data Protection Officer to report to Regulators/Central Bodies, if required.

Final Score	Level of SIRI
1 or less	Level 1 IG SIRI (Not Reportable)
2 or more	Level 2 IG SIRI (Reportable)

Sensitivity Factor Guide (IG SIRI)

(A) No sensitive personal data (as defined by the Data Protection Act 1998) at risk nor data to which a duty of confidence is owed

Example: The data involved in the incident does not contain information that includes:

- Racial or ethnic origin of data subjects
- Political opinions of data subjects
- Data subjects religious beliefs or other beliefs of a similar nature.
- Details as to whether the data subjects are members of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992.
- The physical or mental health or condition of data subjects
- Sexual life of data subjects
- The commission or alleged commission by a data subject of any offence; or
- Any proceedings for any offence committed or alleged to have been committed by a data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Confidential information includes clinical records or any data that would enable someone to learn something confidential about someone that they didn't already know.

Data that is neither confidential nor sensitive will be demographic data that isn't readily available in the context e.g. an individual's name in the context of who was present at a hospital on a particular day.

(B) Information readily accessible or already in the public domain or would be made available under access to information legislation e.g. Freedom of Information Act 2000

Example: The data involved in the incident is already accessible in the public authorities Publication Scheme or otherwise available on the public authorities' website. This could be copies of business meeting minutes, copies of policies and procedures that may contain the name of a senior officer or members of staff responsible for signing off such material where they have an expectation that their names and job titles would be accessible.

Example: Non- confidential information e.g. information from telephone directory which includes data items to which we do not owe a duty of confidence.

(C) Information unlikely to identify individual(s)

Example: Information is likely to be limited demographic data where the address and/or name of data subjects is not included. For example: lists of postcodes within political wards

Examples include Soundex codes, weakly pseudonymised personal data, and Hospital ID number.

(D) Detailed information at risk e.g. clinical/care case notes , social care notes

Example: This would include Social Worker case notes, Social Care Records, Information extracted from core Social Care systems, Minutes of Safeguarding Review Meetings, Hospital discharge data details, observations of service users, clinical records etc.

(E) High risk confidential information

Example: This would include information where disclosure has been prohibited by Order of a Court and may also include information which its disclosure/handling is governed by statutory requirements, guidance or industry Organisation. This may include information processed under the following, but not limited to, publications:

Information classed as particularly sensitive information: Sexually Transmitted Disease (STD), rape victims, child safeguarding data which would cause considerable distress and damage if it got into the public domain.

.

(F) One or more previous incidents of a similar type in the past 12 months

Example: More than one incident where an email containing sensitive or confidential data identifying a living individual, has been sent to the wrong recipient. One or more incidents of Social Workers leaving their case recording books with a User of a service. One or more incident of a fax being sent to the wrong fax number or sensitive prints being left on a printer.

Could include multiple incidents of the same type which have occurred within a specific department or unit or organisation. Specify within the incident details in terms of whether it is a reoccurring problem within a team, department or throughout the organisation.

(G) Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information

Example: Data has been transferred onto an unencrypted USB device in breach of organisational policy and subsequently lost. Disclosure of information because of not complying with an organisations mobile device guardianship policy e.g. left in the car overnight.

Example: GP transferring clinical records on unencrypted CD's. Organisations should have policies in place which reduce the risk of data breaches and to ensure that avoidable risks do not occur or reoccur.

(H) Likely to attract media interest and/or a complaint has been made directly to the ICO by a member of the public, another organisation or an individual
Example: Loss of large volumes of personal identifiable data being shared between a public authority and an outsourced/commissioned provider. Disclosure of information relating to sex offenders or vulnerable adults. Where a complaint has been made to the ICO. They are duty bound to investigate if a data breach has taken place. This type of incident would often receive more attention than would otherwise be the case due to the route by which the breach was raised.

(I) Individuals affected are likely to suffer substantial damage or distress, including significant embarrassment or detriment
Example: Substantial damage would be financial loss e.g. the loss of Bank Account details of service users, likely resulting in the actual loss of funds of a data subject. Substantial distress would be a level of upset, or emotional or mental pain, that goes beyond annoyance or irritation e.g. loss of entire historical record relating to a previously looked after child. Example: Details of individual in witness protection program or individual asked for their ID to be protected.

(J) Individuals affected are likely to have been placed at risk of or incurred physical harm or a clinical untoward incident
Example: Loss of personal information relating to Vulnerable Adults identifying their location, key safe details, reasons for vulnerability. Disclosure of information relating to Data Subjects located in refuge houses, Disclosure of information relating to location of offenders being rehabilitated in the community. Example: Loss of the sole copy of a clinical or social care record. Information where there is no duplicate or back up in existence, so prejudicing continuity of care.