Personal Data Breach Policy

Version Control

Version No.	Date Edited	Edited By	Summary of Changes
1.0	29.3.19	Dawn Hambly	
1.1	29.8.19	Marina Edwards	add version control

Personal Data Breach Policy

Introduction

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. They must do this within 72 hours of becoming aware of the breach.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, they must also inform those individuals without undue delay.

They must also keep a record of any personal data breaches, regardless of whether they are required to notify.

What is a personal data breach?

A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Types of personal data breaches

There are three main categories of personal data breach, which include:

1. Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data;
2. Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data; and
3. Integrity breach - where there is an unauthorised or accidental alteration of personal data.

Examples of personal data breaches

Some examples of personal data breaches may include (but not limited to):

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration, deletion or destruction of personal data without permission; and
- loss of availability or control of personal data;

Reporting Process

The practice will establish whether a personal data breach has taken place and promptly take steps to address it. This will include a decision-making process to report the incident to the Information Commissioner if required.

When a personal data breach has occurred, the practice will to:

1. Minimise the impact of the breach by containing it by implementing any actions deemed appropriate;
2. Undertaking a risk assessment to determine whether the incident requires onward reporting to either the Information Commissioner or to the data subject affected (or both);
3. Ensure recording of all personal data breaches regardless of whether the breach requires onward reporting.

Personal Data Breach Identification & Recording

The practice has set up systems and processes to identify whether a breach has taken place, as well as to assess the significance of the risk. In addition, a system to monitor any breaches has also been developed which are in line with GDPR requirements.

Flow Chart & Risk Assessment

The practice will use the Personal Data Breach flowchart in Appendix A in conjunction with the Risk to Right and Freedom Risk Assessment in Appendix B to identify whether onward notification needs to be made as a result of the breach. In addition, a record of the data breach will be kept in line with monitoring requirements (Appendix C).

The completed template will be sent to the Practice Manager or Information Governance Manager within 24 hours of the incident occurring. The primary focus will be to establish the type of incident and to quickly contain the breach and prevent further adverse effects upon the personal data. It will also allow onward reporting within 72 hours if required.

The risk assessment identifies the likelihood and level of risk that the rights and freedoms of an individual have been affected by the breach. These are highlighted in Recital 75 of GDPR and include the following:

- where the processing may give rise to discrimination, identity theft or fraud
- financial loss
- damage to reputation
- loss of confidentiality of personal data protected by professional secrecy
- unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;
- where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data
- where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership,
- the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;

- where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- where personal data of vulnerable natural persons, in particular of children, are processed;
- where processing involves a large amount of personal data and affects a large number of data subjects.

Monitoring template

The monitoring template has been designed to ensure all personal data breaches are investigated and measures put into place to address and to mitigate the breach. The excel spreadsheet will be completed to ensure a contemporary record of any incidents to learning can be applied and systems and processes improved.

The monitoring template includes a self-populating Excel spreadsheet:

- Date of the incident;
- Date reported to the Practice Manager/IG Manager;
- Whether a Personal Data Breach has occurred;
- Type of Personal Data Breach
- Type of Data Subject
- Type of Data Record
- Number of subjects affected;
- Full description of the incident;
- Assessment of risk to individual rights and freedoms;
- Likelihood of risk
- Risk level
- Severity of risk
- Damage as a result of breach;
- Consequence of breach
- Measures taken to address and mitigate breach;
- Assessment of whether ICO and Patient need to be notified

Outcome of risk assessment

The practice will ensure that all breaches are recorded, regardless of whether or not they need to be reported to the ICO or the Patient as per the arrangements set out under GDPR:

- No Risk to Rights and Freedoms – the breach does not need to be notified to the ICO;

- Risk to Rights and Freedoms – the breach needs to be reported to the ICO;

- High Risk to Rights and Freedoms – the breach needs to be reported to the patient.

To report the breach, the Practice Manager will contact the Information Commissioners Office on the Personal Data Breach helpline on 0303 123 1113 or will complete the online form at

https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/ and send it to casework@ico.org.uk

The practice will report the breach without undue delay and not later than 72hrs after becoming aware of the breach. If the breach is reported later than 72 hours then it shall be done so accompanied by reasons for the delay.

If a breach has been identified, but there is insufficient or incomplete information, the practice will report as much information as is available at that time to the ICO. Further information will be reported to the ICO as it becomes available.

Data Processors

The practice uses multiple data processors. If a processor suffers a breach, then under Article 33(2) it must inform the practice without undue delay as soon as it becomes aware. The processor must comply with any investigation, reporting and remedial actions undertaken or determined by the practice.

Informing Data Subjects

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the practice will inform those concerned directly and without undue delay. In other words, this should take place *as soon as possible*.

Whilst the threshold for informing individuals is higher than for notifying the ICO, the practice will inform data subjects potentially affected if the breach was classified as reportable to the ICO.

The practice will describe to individuals, in clear and plain language:

- the nature of the personal data breach
- the name and contact details of our data protection officer or other contact point where more information can be obtained
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects

The practice will not need to inform data subjects if:

a) the practice *had* 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; and

b) the practice *had* taken *subsequent* measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise

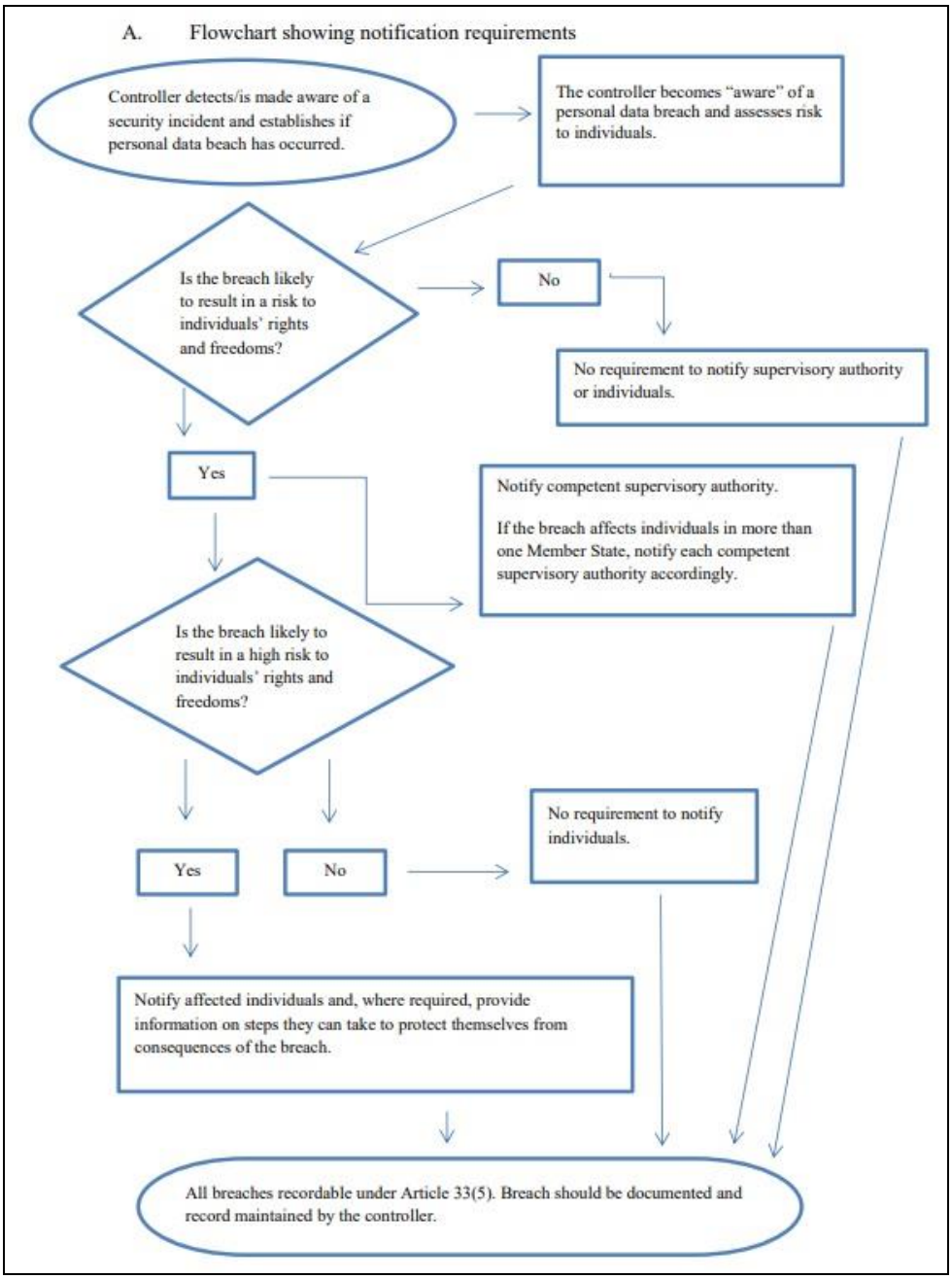
The practice will, however, need to inform data subjects *if the ICO*, having been alerted by the practice's notification, and on reviewing the report, decides that data subjects ought to be informed.

Post breach discussion

The practice will investigate the root cause of the breach and identify how a recurrence can be prevented. Any breaches and all subsequent actions will be discussed at a practice meeting.

Personal Data Breach Flowchart (Appendix A)

In the event of a Personal Data Breach, the practice will follow the flowchart to determine whether the event is reportable to either the ICO (High Risk) or the Patient (Very High Risk).



In addition, a Personal Breach Reporting Template will be completed to ensure adequate reporting of the breach (see below).

Personal Data Breach

A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

In the event of a personal breach

In the event of a personal breach, the practice will examine the extent to which the rights and freedoms of the individual have been affected. The risk assessment will review the likelihood and severity of the risk and this will inform the notification process.

Risks to Rights and Freedoms

Recital 75 of GDPR outlines the circumstances in which risks the rights and freedoms of the individual are affected. These are highlighted as follows:

The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

TestvaleSurgery

Risk to Right and Freedom Risk Assessment (Appendix B)

Risk to Right & Freedom	Likelihood score	Severity Score	Outcome
Discrimination			
Identity theft or fraud			
Financial loss			
Damage to the reputation			
Loss of confidentiality			
Unauthorised reversal of pseudonymisation			
Any significant economic or social disadvantage			
Deprivation of rights and freedoms			
Prevention from exercising control over their personal data			
Reveals racial or ethnic origin			
Reveals political opinions			
Reveals religious or philosophical beliefs			
Reveals trade union membership			
Processing of genetic data			
Data concerning health			
Data concerning sex life			
Data concerning criminal convictions and offences			
Performance at work			
Economic situation			
Health, personal preferences or interests			
Reliability or behaviour			
Location or movements			
In creating or using personal profiles			
personal data of vulnerable natural persons (in particular children)			
Affecting large amount of personal data and affects a large number of data subjects.			

Risk Assessment Matrix

		Likelihood				
		Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Risk Level	**Catastrophic**	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Minor	2	4	6	8	10
	Negligible	1	2	3	4	5

Colour	**Risk level**	**Outcome**
Green	No Risk	Do not report
Amber	Risk	Report to ICO
Red	High Risk	Report to Patient

Personal Data Breach Monitoring Template (Appendix C)

The Personal Data Breach Monitoring Template will be completed by the practice in the event of a personal data breach and this will be used as a contemporaneous log of events which will be used for learning and process improvement.