South, Central and West Commissioning Support Unit

Information Governance Breach

Guidance for Practices

South, Central and West
Commissioning Support Unit

Contents

1. What is an Information Governance breach?

GDPR Article 4 (12) 2 Personal Data Breach" 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.

IG Breaches can be categorised as:

- Confidentiality – unauthorised access or accidental disclosure of personal data.
- Integrity of systems -unauthorised or accidental alteration of personal data
- Availability – accidental loss of access to, or destruction of personal data

2. Confidentiality

Unauthorised or accidental disclosure of or access to personal data;

For example:

- Letters, emails or telephone message, sent or disclosed to the wrong patient, member of public or staff member, organisation
- Failure to secure information contained in a subject access request, lack of redaction
- Prescriptions given to the wrong patient
- Unauthorised access to records, either by hacking or design, i.e. another organisation given access to the GP system without a lawful basis to do so

3. Integrity

Unauthorised or accidental alteration of personal data, a document or consultation could be entered onto the wrong patient record;

For example:

- Records edited or deleted in error
- Misfiling important results or documentation.
- Scanner picks up two different patient letters and accidentally adds them to one patient. This could have consequences to both patients there may be medication changes detailed which are missed on a patient, or treatment information.
- GP pulls up a patient's record, but they DNA – and the next patient comes in for a consultation – GP enters it on the previous patient and issues meds. There could be a serious risk of the patient missing their treatment, or it being prescribed again for the other patient when it should not be their treatment

4. Availability

Unauthorised or accidental loss or access to, or destruction of, personal data, where personal data is unavailable when it should be;

For example:

- Insecure disposal of paperwork or hardware. i.e. documents or diaries containing patient details being thrown in the main dustbin, or laptops or computers being taken to the local waste transfer site.
- Staff confidential HR paperwork left in public area, including financial information and personal details, now missing
- Failure to securely address or send letters to patients or organisations and letter not received.

It is important to remember that it is not just about confidential information being disclosed, or the amount of people effected. It is about the level of harm that can be incurred by the individual whose data has been breached.

Incidents should be graded based on the potential and actual harm incurred by a patient or staff member. All incidents grading over a 6 should be reported to the ICO using the DSP Toolkit. **You should alert your DPO within 24 hours,** so they can discuss it with you and help you grade the breach.

Complete a breach form to ensure that you keep accurate records. (**Appendix A***)*

The initial investigation of the events leading to the breach should be completed within **48 hours**. Breaches that have to be notified to the ICO must be reported within **72 hours** of the breach being realised. It is therefore important that your staff are aware that they must tell someone – your practice protocol should recognise the importance of reporting in a timely way.

5. Near miss

This would be a potential breach which is prevented, or where the data does not leave the practice or the NHS.

For example:

- Receptionist hands patient prescription who then realises that there is one for a different patient slipped in with it – they hand it back before leaving the practice. (*Confidentiality*)
- Secretary emails letter to the wrong department in a hospital – they notify you. (*Confidentiality)*
- Email sent to the wrong nhs.net e-mail address.
- EPS prescription sent to wrong nomination.

The practice should record all breaches, including near misses on a log – complete a significant event and consider what happened, can this be prevented, and/or do you need to change the processes to prevent this happening in future?

Do not assume that there is no (IMPACT) from a near miss – in the case of a prescription being sent to the wrong nominated pharmacy the patient concerned may suffer distress due to having to travel further, have a delay in getting their medication, and there will be an impact from time to sort the situation out. All low level incidents have to be logged and lessons learnt recorded.

The near miss log should contain the date the breach happened, the date it was discovered, the facts of the incident, the effects, who dealt with it and any actions taken.
Do not identify the patient by name or PID – but you can record the clinical system number.
In all cases these incidents should be discussed at practice meetings, and recorded in your minutes.

Document everything, and keep on file as evidence in case you are asked to account for you actions in the future.

6. Third Party Breaches

Practices will receive information from external agencies which is not related to their patients. In this situation you must notify the organisation concerned as soon as possible. It is their responsibility to report the breach and carry out their own process for Duty of Candour and breach investigation.

For example:
You receive information from a pharmacy on health checks they have carried out – in the list of patients one is registered with you – the remaining 5 are registered elsewhere.

Or you receive an unencrypted CD containing patient information, in the post, from an external source such as the MOD – this is an integrity breach and your Caldicott Guardian should write to the MOD explaining that they have breached patient confidentiality, and that you will be unable to process this information – in many cases you may no longer have CD readers, it is putting your system at risk if you introduce information in this way, and as the data is unprotected you would not be able to provide assurance that it has not been viewed by anyone else.

If you contract other organisations to work on your behalf you may receive information regarding breaches made by the third party processor – in this case as data controller – you should regrade the incident, and you would, as data controller, be responsible for reporting this to the DSP Toolkit, or log it on your records.

7. Grading of breaches

When a breach is graded it is based on the level of harm that could potentially (IMPACT) be incurred by the person whose data has been breached, and the (LIKELIHOOD) that actual harm has been incurred.

The breach has to be graded; your DPO can help with this.

DSP IR guidance Sept 2018.pdf

The tables on page 14 of the guidance will help you consider the score for each element. For example, in a prescription breach you must consider the potential harm (IMPACT) from the upset that personal information has been received by another person, through to delaying treatment while the surgery investigate what happened to the original prescription.

Next you look at what actually happened – there may have been no delay in the patient getting their medication, and they may not be distressed that this error occurred. Or it could have been an urgent prescription, they could have been going on holiday so needed it without delay and they may be very upset that another patient now knows what medication they are on. This is not about assuming what the situation was, but determining what actually happened (LIKELIHOOD).

In the situation of a letter going to the wrong patient, the potential harm could be from the upset that personal information has been received by another person, through to delayed treatment resulting in an increase of symptoms or even death.

In some cases, you may not know the full impact of the situation within the time frame for reporting (72 hours) in which case you should consider the potential harm (IMPACT) to be worse case scenario.

When grading the breach the score for the IMPACT is multiplied by the score for the (LIKELIHOOD) and any total score over a 6 must be reported on the DSP Toolkit within 72 hours, in some cases the score may change as you investigate the breach – if it increased from a lower score to above a 6 you need to report it, with an explanation of what happened and why it has changed.

If in doubt you should report it through the DSP Toolkit.

8. Reporting the Breach

The DSP Toolkit has a section for you to report a new incident. You should complete as much information as possible; this will help any breaches which are then escalated to the ICO to be assessed. In most cases, if you have followed your IG Breach protocol, you will be given a log number for your records and it will be closed.

You can go and update the information on the incident, and should do as your process and investigation progresses. Do not tick the box to state that you have completed everything until it has been done.

The ICO need to determine that you understand what processes caused the breach, that you have correct guidance and protocols for your staff to work to, and that you have carried out all required processes to support your patients and protect their data.

Practices have received fines in the past for not having protocols for their staff to follow, and not having support from the data controllers, and policies to ensure that the protocols provide the security and guidance to prevent breaches occurring.

If you are unsure of your processes your DPO will be able to advise you – always ask for advice.

9. Appendix A - Non-clinical risk incident reporting form

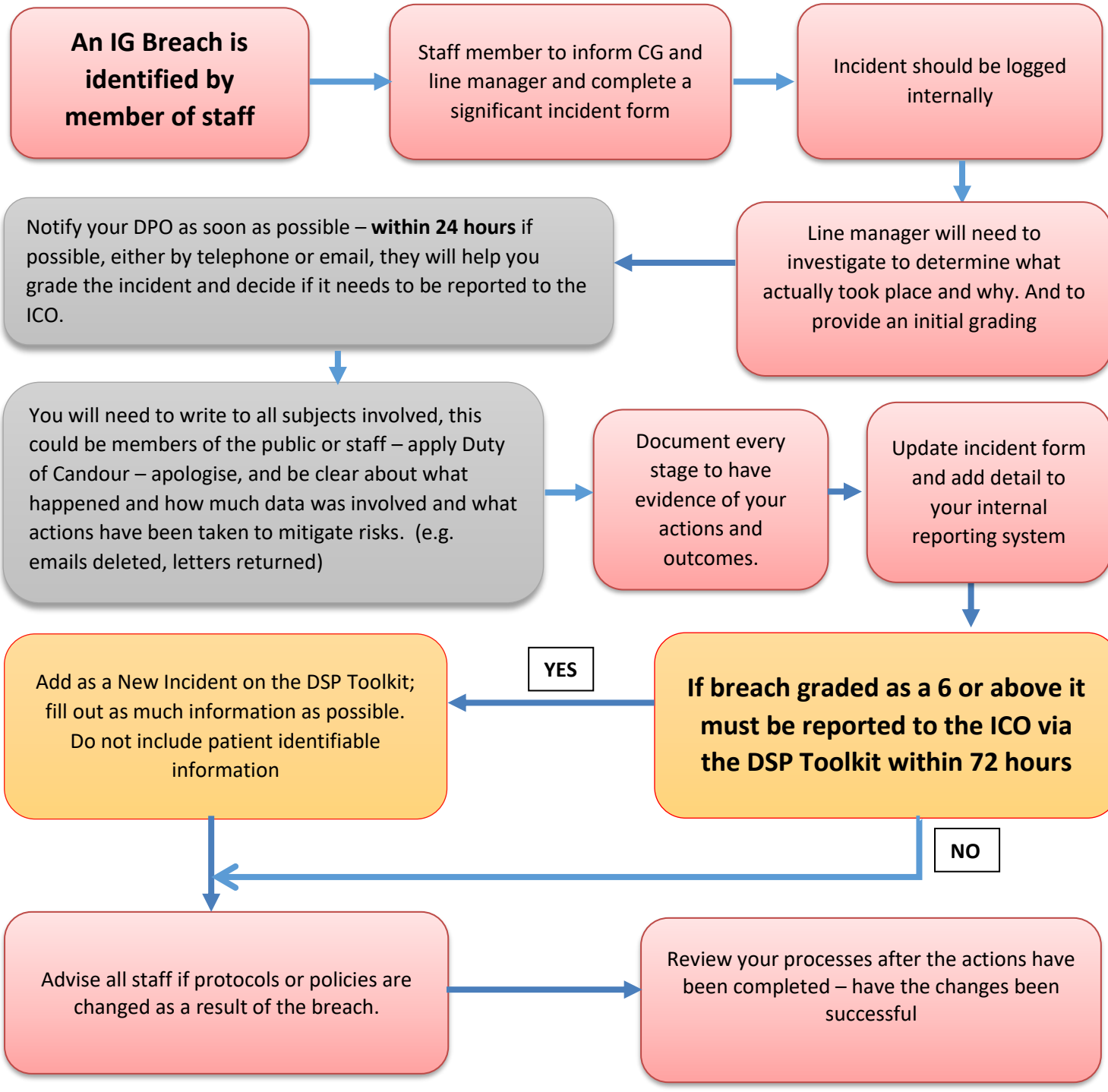
data Breach Incident reporting form.docx

Personal data breaches scoring a 6 or over must be reported to the ICO within 72 hours. Log onto the Data Security & Protection Toolkit (DSPT) to report the breach: https://www.dsptoolkit.nhs.uk

Data breaches must be managed in line with the NHS DIGITAL - Guide to Notification of Data Security & Protection Incidents https://www.dsptoolkit.nhs.uk/Help/29. This also includes information on the considerations for grading the breach; your DPO can discuss this further with you.

South, Central and West Commissioning Support Unit

10. Appendix B - Serious breach notification – Flow Chart



IMMEDIATE ACTION

If a referral letter containing information/medication details or other information was sent to the wrong patient, ensure that it is resent to the correct patient without delay.

11. Document Control

This document was created by NHS South Central and West Commissioning Support Unit (SCW) and as such the IP rights of this document belong to SCW.

Document Name	Version	Status	Author
Information Governance Breaches Guidance for Primary Care	1.0	Published	NHS SCW Information Governance Services
Document objectives:	This document supports Practice staff in compliance with Data Protection legislation, achieving best practice in the area of Information Governance and in meeting the requirements of the Data Security and Protection Toolkit		
Target audience:	All staff		
Monitoring arrangements and indicators:	This document will be monitored by NHS SCW Information Governance Services to ensure any legislative changes that occur before the review date are incorporated.		
Approved and ratified by:	New Wokingham Road Surgery	May 2021	
Date issued:	May 2021		
Date uploaded to Website	May 2021		
Review date:	May 2022		

Change record

Date	Author	Version	Page	Reason for Change
27.08.2020	SCW	1	All	Review for Website publication