NHS Digital

Guide to the Notification of Data Security and Protection Incidents.

Reporting incidents post the adoption of GDPR 25 May 2018 and NIS Directive 10 May 2018

September 2018

Information and technology
for better health and care

Revision History

Version	Date	Summary of Changes
1	25th May 2018	Initial version
1.1	07th June 2018	Updated following comments from users and development of the DSP Toolkit.
1.2	03rd July 2018	Updated following feedback from users and ICO.
1.3	14th September	Update guidance on Annual reports, labels on 5x5 grid and consistency amendments.

Document Status

This is a controlled document. Whilst this may be printed, the electronic version posted on the DSPT is the controlled copy. Any printed copies of the document are not controlled.

Contents

Overview

The General Data Protection Regulation (GDPR) as implemented by the UK Data Protection Act 2018 comes 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. The Security of Network and Information Systems Directive ("NIS Directive") also requires reporting of relevant incidents to the Department of Health and Social Care (DHSC) as the competent authority from 10 May 2018.

An organisation must notify a breach of personal data within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of individuals, organisations must also inform those individuals without undue delay. Those breaches that also fulfil the criteria of a NIS notifiable incident will be forwarded to the DHSC where the Secretary of State is the competent authority for the implementation of the NIS directive in the health and social care sector. The Information Commissioner remains the national regulatory authority for the NIS directive.

For urgent security related incidents that require immediate advice and guidance an organisation is advised to contact the Data Security Centre (formerly known as CareCERT) helpdesk immediately on 0300 303 5222 or contact enquiries@nhsdigital.nhs.uk

Organisations should ensure robust breach detection, investigation and internal reporting procedures are in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

It remains a contractual requirement of health and social care organisations using the standard NHS contract to include statistics on personal data breaches in the annual report presented to the board.

Organisations must also keep a record of any personal data breaches, regardless of whether it is required to notify. It must not include the identity of any person involved in a data breach in a notification. The local file may contain such information, but this file will only be requested by the Information Commissioner (ICO) if further investigation is required.

This guidance applies to all organisations operating in the health and care sector with a very few exceptions listed below. This includes all organisations registered with the Care Quality Commission (CQC) and those organisations processing health and social care personal data under contract with the health and social care sector including directly commissioned services and their support services. By health and social care sector this includes all NHS services and those in contract with the NHS and adult social care services.

Certain other organisations have the option of using this notification tool such as private health and social care services that are not contracted by a public sector organisation and those parts of local government not delivering adult social care services. Personal data breaches that fall out of scope can be reported either via this reporting tool or to the Information Commissioner directly at the discretion of the reporting organisation. However, those organisations already using the Data Security and Protection Toolkit (DSPT) may find it easier to use a reporting tool that is already at their disposal.

This guide supersedes the 'Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation' (2015). This reporting tool is not designed to be a fully functional incident management system. It is for the purposes of notifying breaches on one form which may then be shared across several regulatory agencies. These include personal data breaches of the GDPR to the Information Commissioner, NIS incidents to the DHSC and cyber security incidents to NHS Digital. Organisations must maintain a local file or use an incident management system to fully record the particulars of any investigation and remedial action. Notifications should include as much detail as is available to allow a full assessment by the ICO and other regulatory organisations. Failure to include sufficient detail in notifications will trigger further prompts for more information which may come from multiple regulatory bodies.

This guidance has been developed with the ICO, DHSC, NHS England, NHS Digital and NHS organisations.

Mandate

General Data Protection Regulation as Implemented by the Data Protection Act 2018 (GDPR)

It is a legal obligation to notify personal data breaches of the GDPR under Article 33 within 72 hours, to the ICO, unless it is unlikely to result in a risk to the rights and freedoms of individuals. Article 34 also make it a legal obligation to communicate the breach to those affected without undue delay when it is likely to result in a high risk to individuals rights and freedoms. It is also a contractual requirement of the standard NHS contract to notify incidents in accordance with this guidance. By notification this may be an initial summary with very little detail known at the outset but a fuller report that might follow. There is no expectation that a full investigation will be carried out within 72 hours. The ICO has asked all relevant health and social care organisations to use this reporting tool accessed via the DSPT in preference to the ICO provided reporting mechanism so that sector intelligence gathering and local solutions to groups of incidents can be implemented.

A processor of personal data that discovers a breach has occurred has a legal obligation to inform the controller of that personal data under Article 33(2) of GDPR as clarified in the Article 29 working party guidelines on personal data breach reporting. It is possible for a processor to make a notification on behalf of the controller, but only where the controller has authorised the notification and this has been documented as part of the contractual arrangements between the controller and the processor. However, it is important to note that the legal obligation remains with the controller.

ICO currently advise the following relating to reporting health and care sector incidents - ‘All health service organisations in England must now use the IG Toolkit Incident Reporting Tool. This will report IG SIRIs to the NHS Digital, DHSC, ICO and other regulators.’ (The IG Toolkit is now replaced with the DSPT).

Security of Network Information Systems Regulations 2018 (NIS)

The Security of Network and Information Systems Regulations 2018 (“NIS Regulations”) 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’.

Incidents must be reported without undue delay, and in any event within 72 hours of the operators of essential services becoming aware of the incident.

For purposes of the NIS Regulations for the health sector in England:

I. the competent authority is the Secretary of State for Health and Social Care (i.e. the DHSC);

II. operators of essential services are NHS Trusts, NHS Foundation Trusts, and any other person designated by the Secretary of State for Health and Social Care; and

III. the criteria for events which have a 'significant impact' on the continuity of essential services which must be reported under the NIS Regulations are set out at page 10 of this guidance.

The Secretary of State for Health and Social Care requires that this incident reporting tool should be used for the reporting of incidents under the NIS Regulations.

The requirement to report events which have a significant impact on the continuity of essential services under the NIS Regulations (in the health sector in England) applies only to NHS Trusts, NHS Foundation Trusts, and any other person designated by the Secretary of State for Health and Social Care. Any person designated as an operator of essential services for the purposes of the NIS Regulations by the Secretary of State for Health and Social Care will be notified of that designation.

Transitional arrangements

Data breaches that originated before 25 May 2018 and subsequently have come to light after this date must be reported on the Data Security and Protection Incident Reporting Tool. If an organisation is unsure then use this tool and the regulatory authority will make a determination as to which legal framework applies i.e. Data protection Act 1998 or GDPR. The previous version of the SIRI tool will remain available for use after this date for a period to complete unreported incidents. Previously reported incidents will still be available in a read-only format for at least 7 years after 25 May 2018 for purposes of legal compliance.

NIS reportable incidents must be reported from 10 May 2018.

Personal Data Breaches

What is a breach

A breach is defined as;

Article 4(12) “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.

Breach reporting is now mandatory for all organisations. The GDPR definitions, notification and subject communication requirements will include breaches that organisations might not have notified under the previous data protection regime. The traditional view that a data breach is only reportable when data falls into the wrong hands is now replaced by a concept of a ‘risk to the rights and freedoms of individuals’ under Article 33 of GDPR. Any security breach that creates a risk to the rights and freedoms of the individual is a personal data breach and could be notifiable to the ICO if it reaches a certain threshold. Any personal data breach that could create a significant risk to the rights and freedoms of an individual must be notified to the Information Commissioner via this reporting tool. All personal data breaches will involve a breach of security at some point in the processing and the additional use of this tool for NIS incident reporting will save the health and social care sector time and effort in reporting.

Personal data is defined as;

‘any information relating to an identified or identifiable living individual’

And an “Identifiable living individual” means a living individual who can be identified, directly or indirectly, by reference to— (a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

This definition now makes it clear that all paper records that relate to a living individual are included in the definition and any aspect of digital processing such as IP address and cookies. Geographical data and biometric data are also clarified as being personal data when they can also be linked to a living individual.

If it is still unclear when to notify there are some examples of personal data breaches at the end of this guide.

What are the types of breaches

The three types of breaches as defined in the Article 29 Working Party on Personal data breach notification are Confidentiality, Integrity or Availability (CIA).

The CIA Triad

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

Confidentiality breach example

Unauthorised or accidental disclosure of, or access to personal data – Infection by ransomware (malicious software which encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals. If the attacker has not accessed personal data, the breach would still represent an availability breach and require notification if the potential for a serious impact on the rights and freedoms of the individual.

Availability breach example

Unauthorised or accidental loss of access to, or destruction of, personal data - In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled. This is to be classified as an availability breach.

Integrity breach example

Unauthorised or accidental alteration of personal data – Where a health or social care record has an entry in the wrong record (misfiling) and has the potential of significant consequences it will be considered an integrity breach. For example, a 'do not resuscitate' notice on the wrong patient record may have the significant consequence of death whilst an entry recording the patient blood pressure may not have the same significant result.

When is an incident reportable under GDPR

Grading the personal data breach

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation. It is advisable that incidents are reviewed by the Data Protection Officer or Caldicott Guardian or the Senior Information Risk Owner when determining what the significance and likelihood a data breach will be.

The significance is further graded rating the incident of a scale of 1-5. 1 being the lowest and 5 the highest.

The likelihood of the consequences occurring are graded on a scale of 1-5 1 being a non-occurrence and 5 indicating that it has occurred.

Where the personal data breach relates to a vulnerable* group in society, as defined below, the minimum score will be a 2 in either significance or likelihood unless the incident has been contained. This will have the effect of automatically informing the Information Commissioner if one of the other axes scores above a 3.

Where vulnerable is a 'Child known to safeguarding or with mental health conditions. Adult with capacity issues or known to adult safeguarding'.

Establish the likelihood that adverse effect has occurred

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

If the likelihood that an adverse effect has occurred is low and the incident is not reportable to the ICO, no further details will be required.

Grade the potential severity of the adverse effect on individuals

No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job

No.	Effect	Description
		such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

Both the adverse effect and likelihood values form part of the breach assessment grid.

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.

Under the following circumstances notification may not 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.
- cancel the effect of a breach - where the controller can null the effect of any personal data breach.

Example of how the ‘trusted’ partner can be used to contain a breach

There may be a confidentiality breach, whereby personal data is disclosed to a third party or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them and it may be aware of their procedures, history and other relevant details, the recipient may be considered “trusted”. In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with

its recovery.

In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller must keep information concerning the breach as part of the general duty to maintain records of breaches.

Breach Assessment Grid

This operates on a 5 x 5 basis with anything other than “grey breaches” being reportable. Incidents where the grading results are in the red are advised to notify within 24 hours.

Severity (Impact)	Catastrophic	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	No adverse effect	1	1	2	3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood that citizens' rights have been affected (harm)				

DHSC & ICO

ICO

Or in narrative

Where the incident is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor, the incident is reportable and full details will be automatically emailed to the ICO and the NHS Digital Data Security Centre.

The DHSC will also be notified where it is (at least) likely that harm has occurred and the impact is at least serious.

Sensitivity Factors

Sensitivity factors have been incorporated into the grading scores. If a breach involves certain categories of special categories/vulnerable groups it must be assessed as at least:

A Likelihood of 'Not likely or incident involved vulnerable groups (where no adverse effect occurred)' Not Likely on the grid.
and
A Severity of 'Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred'. Minor on the grid.

So even where an incident involves special categories/vulnerable groups, on the breach assessment grid above, it would be a minimum of 4 and so would not be always be reported to the ICO. It would be reported to the ICO if the Likelihood of harm is assessed as at least 'Likely'.

Special Categories of personal data

For clarity special categories under GDPR are;
- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- and the processing of genetic data,
- biometric data for uniquely identifying a natural person,
- data concerning health,
- data concerning a natural person's sex life or sexual orientation

For clarity special categories under GDPR not listed above include;

- Vulnerable children
- Vulnerable adults
- Criminal convictions/prisoner information
- Special characteristics listed in the Equality Act 2010 where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or individual
- Communicable diseases as defined by public health legislation
- Sexual health
- Mental health

Criminal convictions and offences under Article 10 of the GDPR is further explained in the Data Protection Act 2018 Part 2, Chapter 2, S10 (2) and also includes -

(a) the alleged commission of offences by the data subject;
or
(b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

Assessing risk to the rights and freedoms of a data subject (likelihood)

The GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

Depending on the outcome of the scoring matrix contained in this guide the risk may be high risk and be significant enough to notify to the ICO. If there is any doubt that a breach is significant enough for notification it is always best to notify.

A tabular conversion table at Appendix 4 lists how previous data breach reporting maps to the GDPR categorisations. A full list of rights and freedoms is given at the following link and the above are a summary of the main results of a breach on those rights.

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

What to include in the notification

Article 34 of the GDPR outlines what must be communicated to the relevant authority and this has been included in this reporting tool.

The GDPR requires that the following information be included in any notification;

- a description of 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.

- the name and contact details of the data protection officer or other contact point from whom 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 by the

controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Events having a Significant Impact on the Continuity of Essential Services (NIS Regulations)

Who the NIS Regulations apply to

The requirement to report events which have a significant impact on the continuity of essential services under the NIS Regulations (in the health sector in England) within 72 hours applies only to NHS Trusts, NHS Foundation Trusts, and any other person designated by the Secretary of State for Health and Social Care. Any person designated as an operator of essential services for the purposes of the NIS Regulations by the Secretary of State for Health and Social Care will be notified of that designation.

Any incident reportable under the NIS Regulations may also be reportable as a personal data breach under the GDPR reporting requirements set out in this guidance. Where this is the case the [incident reporting tool] will ensure that the incident is reported to both the ICO and the DHSC. When an incident is reported under both the NIS Regulations and GDPR the Department of Health and Social Care will work with the ICO to ensure appropriate consistency of approach and avoid unnecessary duplication.

This section of the guidance is not relevant to organisations who are not considered operators of essential services for the purposes of the application of the NIS Regulations to the health sector in England as outlined above. However, any data, network or information system incident affecting the delivery of health or social care services is likely to be reportable as a personal data breach in line with the GDPR reporting requirements set out in this guidance.

Significant Impact Thresholds

Category	Criteria	Applies to	Rationale
Excess fatalities[1]	>0	All	Public safety

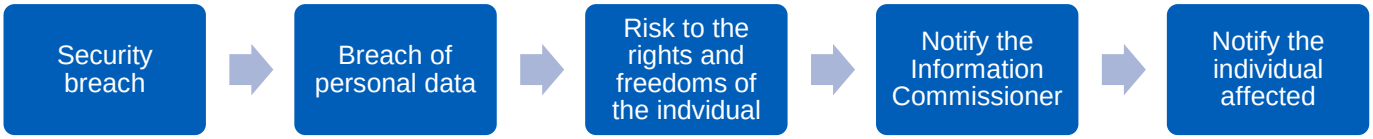
[1] This impact category relates to unexpected/additional fatalities caused by the impact of a network and information systems event. This category covers excess fatalities that occur immediately as a direct result of the relevant event.

Excess casualties[2]	>0	All	Public safety
Potential clinical harm[3]	>50	All	Public safety
Closure or diversion of emergency departments – major trauma centre	>3hrs	Trust – major trauma centre	10% of population, 3 hours
Closure or diversion of emergency departments – all other orgs	>24hrs	Trust/independent provider – non major trauma centre	City, 1% of population, 24hrs
Outpatient appointments cancelled	1,500	Trust/independent provider	City, 1% of population, 12hrs
Inpatient episodes cancelled	250	Trust/independent provider	City, 1% of population, 12hrs
Lack of availability of NHS111 services[4]	>3hrs	NHS111 services	Region, 4% of population, 3hrs
Disruption to NHS emergency ambulance services	(a) ≥85% service degradation for ≥15 minutes (b) ≥30% degradation for ≥35 minutes (c) ≥5% for ≥4 hours	Ambulance	Ambulance Quality Indicators
Non-availability of drugs and/or medical devices	>24hrs	Trust/independent provider	City, 1% of population, 24hrs
Community care appointments cancelled	1,500	Trust/independent provider	City, 1% of population, 12hrs

Further details about NIS are available: on:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/706613/network-and-information-systems-regulations-2018-health-sector-guide.pdf

[2] [This impact category relates to unexpected/additional casualties caused by harm that is attributable to the impact of a network and information systems event. This category covers excess casualties that occur immediately as a direct result of the relevant event.
[3] This threshold reflects the fact that disruption to essential health services creates the risk of clinical harm to patients, and this is something that should be considered in notification of incidents under NIS on patient safety grounds. The figure refers to the number of patients put at risk of clinical harm immediately as a direct result of the relevant event.
[4] This may include call handling operation and/or interfacing services.

How to report an incident summary



Incident Management and breach reporting

Breach reporting may form part of an ongoing incident management or it may be historical. The steps to breach reporting should be complimentary to incident management and not in replacement of it. The DSP Incident Reporting Tool should not be used in place of an incident management process. It is solely for the purposes of reporting to the relevant regulatory authority. There is a legal requirement to maintain a local file containing the particulars of the breach and subsequent investigation and action, if any.

Details of the incident management process in relation to an organisation's responsibility under the data security standards (Data Security Standard 6 Responding to Incidents) is available here:

https://www.dsptoolkit.nhs.uk/Help

How to report an incident

Using the Data Security and Protection Incident Reporting Tool has been designed so that organisations can notify incidents without having to study detailed guidance.

Notifiable breaches are those that are likely to result in a high risk to the rights and freedoms of the individual (data subject). The scoring matrix used in this incident reporting tool has been designed to identify those breaches that meet the threshold for notification. However, there are also a number of breaches of security that are also reportable under NIS which must also be recorded on this tool even if organisations believe they are not notifiable for GDPR.

When to report within 72 hours

The GDPR Article 33 requires reporting of a breach within 72 hours. For urgent security related incidents that require immediate assistance and support an organisation is advised to contact the Data Security Centre (formerly known as CareCERT) helpdesk immediately on 0300 303 5222 or contact enquiries@nhsdigital.nhs.uk . As previously stated, this tool is for notification and local incident management must still be carried out.

This 72 hours starts when an organisation becomes aware of the breach which may not necessarily be when it occurred. An organisation must have a reasonable degree of certainty that a security incident has occurred and that this has led to personal data being compromised. This means that once a member of staff or the public has reported a breach this is the point that an organisation is aware. The actual incident may have occurred some hours, days or weeks previously, but it is only when an organisation is aware that the breach has occurred that the 72 hours to notification period starts. Where the 72 hours deadline is not met an organisation must provide an explanation. Failure to notify promptly may result in additional action by the ICO in respect of GDPR.

In the event that the Data Security and Protection Incident Reporting Tool is unavailable, users may choose to either report the incident via the ICO helpline on: 0303 123 1113 (ICO normal opening hours are Monday to Friday between 9am and 4.30pm).

Or
report when the Data Security and Protection Incident Reporting tool is available noting the reasons for delay in the relevant part of the form.

What to expect once the incident reported

Once an incident meets the threshold for reporting as described in the section ‘When is an incident reportable under GDPR’ and is reported using the Data Security and Protection Incident Reporting Tool a notification message is presented on the Incident Reporting screen displaying:

- ‘Incident Reported’
- confirmation that the ICO has been informed and
- an incident reference number from the incident reporting tool

Shortly after the incident has been reported the reporting organisation will receive:

- an email from the ICO to confirm receipt of the notification and
- an ICO case reference number

This ICO case reference number should be quoted in any correspondence with the ICO in relation to the incident as this is the key reference used by the ICO.

Up until the incident has been reported and notified the incident maybe edited in the Data Security and Protection Incident Reporting Toolabout. However, once reported, the incident can no longer be edited. It will be displayed on the Incident Reporting screen and be available in **read-only** format.

Any updates to the incident should be notified to the ICO by email, quoting the ICO case reference number.

What to expect if an incident is not reportable to the ICO/DHSC

If after completing the assessment of likelihood of impact to citizens' rights and freedoms, the impact of the incident does not meet the threshold for reporting, then the incident will not be reported to the ICO and DHSC and no further information is required. Organisations are not required to record all non ICO/DHSC notifiable breaches on the tool, but this function is available if required.

The incident reference will be displayed and a record will be stored on the Reporting an Incident screen in a read-only format. Once the incident is in read-only format, if more information becomes available about the incident which would make the incident reportable, then a new incident should be reported.

Local records required for an incident notified to the ICO

A local file, which may be requested by the Information Commissioner, must be maintained which must contain the following sections;

- the facts relating to the breach.
- its effects.
- the remedial action taken.

The local file of the investigation may be an incident management system such as those commonly in use throughout the care sector. It may be in any format but if requested by the regulator such as the Information Commissioner it must be passed to them.

Other bodies involvement

This personal data breach reporting tool will forward to the appropriate organisation indicated in the scoring matrix. Additionally, these organisations may have obligations to work with other agencies, such as the National Cyber Security Centre, for example, and any incident may be shared onward. For this reason, it is prohibited to include individual information that could identify any person affected by a breach. Sharing personal data breach incidents between relevant organisations will streamline the sharing of breaches. All incidents will be shared on a quarterly basis in aggregate form for incident monitoring and trend analysis between the organisations listed below. However, for other incidents indicated below the entire incident will be shared immediately with the relevant National regulatory body.

ICO

Any incident graded above as notifiable to the ICO will result in the incident being forwarded to the Information Commissioner. The Information Commissioner will then decide if any action is necessary. In addition, a separate assessment of any self-assessed severity scoring done by the use of this reporting tool will be made by the ICO.

Department of Health and Social Care

Any incident that scores more than a 3 on both axes on the scale will be immediately reported to the Department of Health and Social Care so that the relevant officials can be made aware of any breach that is likely to have an impact on service users and the running of the health and social care sector. Additionally, all incidents that may have an impact on national critical infrastructure as defined by the NIS directive.

NHS Digital

As well as hosting the Data Security and Protection Incident Reporting Tool the information contained within reported breaches may be used as intelligence especially when there could be an effect on the system and services it provides which are relied upon across the sector. NHS Digital will not edit the notification, nor will NHS Digital become involved in the investigation of a personal data breach. NHS Digital will provide a support function for the notification tool and may need to access information and hold support records of their activity. NHS Digital will itself use the notification tool for any personal data breaches that occur where it is the data controller.

NHS England

Any incident that scores more than a 3 on the scale will be reported to NHS England to help inform operational delivery and future commissioning arrangements.

Communication of a personal data breach to the data subject

Article 34 of GDPR requires any personal data breach, that is likely to result in a high risk to the rights and freedoms of individuals, to be communicated with those affected.

Any communication must contain the following four elements

- a description of the nature of the breach;
- the name and contact details of the data protection officer or other contact point from whom 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 by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

A communication is not necessary in the following three circumstances

- the controller has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the breach for example the data were encrypted.
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms if individuals is no longer likely to materialise.
- it would involve a disproportionate effort. However, there is still an obligation to have a communication by another means such as a press notice or statement on the organisation website.

The ICO has produced a guide which may be found on its website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

If an organisation decides not to notify individuals, it will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. The ICO has the power to compel organisations to inform affected individuals if it considers there is a high risk. Organisations should document their decision-making process in line with the requirements of the accountability principle.

Appendix 1 - Glossary

Citizen - Any person or group of people. This would include patients, service users, the public, staff or in the context of incident reporting, any anyone impacted by the incident.

Damage - “Damage” should also be relatively clear: this is where personal data has been altered, corrupted, or is no longer complete.

Destruction - What is meant by “destruction” of personal data should be quite clear: this is where the data no longer exists, or no longer exists in a form that is of any use to the controller.

Loss - In terms of “loss” of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession.

Personal Data Breach - “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”

Unauthorised processing - unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

Vunerable - ‘Child known to safeguarding or with mental health conditions. Adult with capacity issues or known to adult safeguarding’.

Appendix 2 - Useful resources

Personal data breaches: Information Commissioners Office

The Guide to the GDPR explains the provisions of the GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Data Security Standard 6 Responding to Incidents: NHS Digital

Guidance on the management of incidents in line with the data security standards is available here:
https://www.dsptoolkit.nhs.uk/Help/29

Appendix 3 – Dos and Don'ts

Dos:

Do notify personal data breaches as soon as possible within 72 hours that meet the criteria of seriousness and likelihood with as much information you know at the time.

Do continue to treat and manage incident management process to its completion. This may include means of preventing future breaches.

Do update the ICO if your understanding of it alters especially regarding the breach assessment grid.

Do Notify the individual concerned so they can take appropriate action, if necessary.

Please give feedback on the incident reporting tool and guidance using the Feedback link on the DSPT Home Page to help and inform future development direction

If Users of the tool or members of the public would like to propose any changes in future we would welcome suggestions and ideas through the change request form available via exeter.helpdesk@nhs.net

Don'ts

Don't delay in reporting an incident if you are unsure on whether to report– if in doubt err on the side of caution and **notify.**

Don't put anything in the report that could be considered personal confidential data (such as patients / service user details)

Don't expect an operational response and help (such as with a cyber related breach). If you require immediate advice and guidance related to a cyber security incident, please contact the NHS Digital Data Security Centre on: 0300 303 5222.

Appendix 4 - Reporting schema for data breaches from 25 May 2018

The questions asked of organisations reporting an incident are:

ID	Information Requested
1	Organisation Name
2	Organisation Code
3	Name of the person Submitting incident
4	Email Address of person Submitting incident
5	Sector
6	What has happened?
7	How did you find out?
8	Was the incident caused by a problem with a network or an information system?
9	What is the local ID for this incident?
10	When did the incident start?
11	Is the incident still on going?
12	Have data subjects or users been informed?
13	Is it likely that citizens outside England will be affected?
14	Have you notified any other (overseas) authorities about this incident?
15	Have you informed the Police?
16	Have you informed any other regulatory bodies about this incident?
17	Has there been any media coverage of the incident (that you are aware of)?
18	What other actions have been taken or are planned?
19	How many citizens are affected?
20	Who is affected?
21	What is the likelihood that people's rights have been affected?
22	What is the severity of the adverse effect?
23	Has there been any potential clinical harm as a result of the incident?
24	Has the incident disrupted the delivery of healthcare services?
25	Which of these services are operated by your organisation?

The table below incorporates the Article 29 working party categorisation of confidentiality, integrity and availability breaches against the historic SIRI and cyber SIRI classifications. Additionally, the last column has the current ICO categorisations for illustration in a like for like comparison of old to new.

Type of breach Art 29 WP	Sub type Art 29 WP	SIRI tool	Cyber SIRI tool	ICO categorisation including new cyber breach types
Confidentiality				
	Unauthorised or accidental disclosure	B Disclosed in Error	Phishing emails	Data sent by email to incorrect recipient
		H Uploaded to website in error	Social Media Platforms	Data posted or faxed to incorrect recipient
		J Unauthorised Access/Disclosure	Spoof website	Failure to redact data
			Cyber bullying	Information uploaded to webpage
				Verbal disclosure
				Failure to use bcc when sending email
				Data sent by email to incorrect recipient
				Cyber security misconfiguration (e.g. inadvertent publishing of data on website; default passwords)
				Cyber incident (phishing)

	Unauthorised or accidental access	I Technical security failing (including hacking)	Hacking	Insecure webpage (including hacking)
		J Unauthorised Access/Disclosure		Cyber incident (key logging software)
Availability				
	Unauthorised or accidental loss	A) Corruption or inability to recover electronic data	Denial of Service (DOS)	Loss or theft of paperwork
		C Lost In Transit		Loss or theft of unencrypted device
		D Lost or stolen hardware		Loss or theft of only copy of encrypted data
		E Lost or stolen paperwork		Data left in insecure location
				Cyber incident (other – DDOS etc.)
				Cyber incident (exfiltration)
				Cryptographic flaws (e.g. failure to use HTTPS; weak encryption)
	Unauthorised or accidental destruction	F Non-secure Disposal – hardware	Malicious internal damage	Insecure disposal of paperwork
		G Non-secure Disposal – paperwork		Insecure disposal of hardware

Integrity				
	Unauthorised or accidental alteration	K Other	Web site defacement	Other principle 7 failure
				Cyber incident – unknown (e.g. data published on Pastebin but no information on how compromise occurred)

Appendix 5 - Examples of notification

Q. Loss of 250,000 anonymised patients' records used to map clusters a range of conditions related to geography.

A. No provided the data is truly anonymised it's not personal however we would advise confirmation of the information used for mapping (a full postcode with rare conditions would be identifiable or not truly anonymised).

Q. A loss of one patient's scanned in case notes which is likely to lead to problems in treating that patient.

A. Yes as it has caused harm to that individual from a problem in treatment that has arisen from the unavailability of the case notes.

Q. A cyber incident similar to the WannaCry incident of 2017, where there is a determination no data has been lost but encrypted and it affects clinical services.

A. Yes as it effects availability and has a ICO effect on individuals which is likely to result in a risk to individual from cancelled appointments and operations which may prolong the pain and suffering of the patient.

Q. 10 DNA profiles (biometric data) with names sent to the wrong email address.

A. Yes as it may cause harm to the individual unless it is a trusted source or encrypted. The biometric data is a special category of data under GDPR and the combination of a name makes it personal data.

Q. A log of IP addresses and user names who have accessed a patient portal accidently backed up to a cloud provider in Canada

A. No. As the user name could be identifiable and IP addresses are classified as personal data it is a personal data breach. It may score as a non ICO notifiable personal data breach as there is a low risk to the rights and freedoms of individuals.

Q. A medical record of a safeguarded child in a mental health unit are sent to the wrong department of the same hospital trust. No serious adverse effect to the rights and freedoms of the child are reported and at no time has the medical record been unaccounted for or any non 'trusted' person had the opportunity to access the record.

A. No. Although there has been an error and the medical records have not been sent to the correct department this does not need reporting because the department is considered 'trusted'. If the records were sent to another organisation that does not meet the definition of 'trusted' it would be notifiable. An investigation must still be performed, and measures introduced to prevent a further breach.

Q. A set of case notes found in a bin outside a supermarket.

A. Yes a data breach is still a breach irrespective of media. It is not restricted to digital information and continues to include paper-based records.

Q. A single ward handover sheet is found in the hospital car park identifying patients and conditions. It is found by a staff member and is classed as ‘trusted’ and the breach has been contained.

A. Yes as there is a potential breach of patient confidentiality that may have occurred during the time it has been left unattended it just may not be notifiable to the ICO. An organisation must investigate the breach and promote measures, so the breach does not occur again such as training for the team that has been responsible for the breach.

Q. A pathology system has gone down and test results are not available leading to a potential of cancelled operations. No reported harm has occurred yet.

A. Yes the significance of a loss of test results may cause harm to an individual through a cancelled operation. Even if none are reported the NIS threshold means that the pathology system is a key system for the NHS and is reportable. The notification tool will ask additional questions to determine that the pathology system is a critical system for NIS purposes.

Appendix 6 Publishing details of DSP Incidents in Annual Reports and Statements of Internal Control (SIC)

Principles

The reporting of data security incidents in the Annual Report should observe the principles listed below. The principles support consistency in reporting standards across Organisations while allowing for existing commitments in individual cases.

a) You must ensure that information provided on personal data related incidents is complete, reliable and accurate.
b) You should review all public statements you have made, particularly in response to requests under the Freedom of Information Act 2000, to ensure that coverage of personal data related incidents in your report is consistent with any assurances given.
c) You should consider whether the exemptions in the Freedom of Information Act 2000 or any other UK information legislation apply to any details of a reported incident or whether the incident is unsuitable for inclusion in the report for any other reason (for example, the incident is sub judice and therefore cannot be reported publicly pending the outcome of legal proceedings).
d) Please note that the loss or theft of removable media (including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats) upon which data has been encrypted to the approved standard, is not a Serious Incident Requiring Investigation unless you have reason to believe that the protections have been broken or were improperly applied.
e) Incidents designated as “pure Cyber” are not required to be included in the annual reports and SIC at this time. However cyber incidents that are also IG SIRIs should be included.

Content to be included in Annual Reports

Incidents reportable to the ICO and/or DHSC should be included in the Annual Report.

These incidents need to be detailed individually in the annual report in the format provided as Table 1 below. All reported incidents relating to the period in question should be reported.

Table 1
Summary of Data Security and Projection Incidents reported to the ICO and/or DHSC

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

Statement of Internal Control (SIC) Guidance

It is important to remember that an organisation's assets include information as well as more tangible parts of the estate. Information may have limited financial value on the balance sheet, but it must be managed appropriately and securely. All information used for operational purposes and financial reporting purposes needs to be encompassed and evidence maintained of effective information governance processes and procedures with risk based and proportionate safeguards. Personal and other sensitive information clearly require particularly strong safeguards. The Accountable Officer and the board need comprehensive and reliable assurance from managers, internal audit and other assurance providers that appropriate controls are in place and that risks, including information and reporting risks, are being managed effectively.

The SIC should, in the description of the risk and control framework, explicitly include how risks to information are being managed and controlled as part of this process. This can be done for example by referencing specific work undertaken by your organisation and by reference to your organisation's use of the Data Security and Protection Toolkit. The SIC will then be reflected formally in your Annual report.

Any data security and protection incidents reported to the ICO and/or DHSC should be reported in the SIC as a significant control issue.