- Failures in the security, integrity, accuracy or availability of information often described as data loss and/or information governance related issues (see Appendix 2 for further information);
- Property damage;
- Security breach/concern;[12]
- Incidents in population-wide healthcare activities like screening[13] and immunisation programmes where the potential for harm may extend to a large population;
- Inappropriate enforcement/care under the Mental Health Act (1983) and the Mental Capacity Act (2005) including Mental Capacity Act, Deprivation of Liberty Safeguards (MCA DOLS);
- Systematic failure to provide an acceptable standard of safe care (this may include incidents, or series of incidents, which necessitate ward/ unit closure or suspension of services[14]); or
- Activation of Major Incident Plan (by provider, commissioner or relevant agency)[15]

- Major loss of confidence in the service, including prolonged adverse media coverage or public concern about the quality of healthcare or an organisation[16].

1.1. Assessing whether an incident is a serious incident

In many cases it will be immediately clear that a serious incident has occurred and further investigation will be required to discover what exactly went wrong, how it went wrong (from a human factors and systems-based approach) and what may be done to address the weakness to prevent the incident from happening again.

Whilst a serious outcome (such as the death of a patient who was not expected to die or where someone requires on going/long term treatment due to unforeseen and unexpected consequences of health intervention) can provide a trigger for identifying serious incidents, outcome alone is not always enough to delineate what counts as a serious incident. The NHS strives to achieve the very best outcomes but this may not always be achievable. Upsetting outcomes are not always the result of error/ acts and/ or omissions in care. Equally some incidents, such as those which require activation of a major incident plan for example, may not reveal omissions in care or service delivery and may not have been preventable in the given circumstances. However, this should be established through thorough investigation and action to mitigate future risks should be determined.

Where it is not clear whether or not an incident fulfils the definition of a serious incident, providers and commissioners must engage in open and honest discussions to agree the appropriate and proportionate response. It may be unclear initially whether any weaknesses in a system or process (including acts or omissions in care)

[12] This will include absence without authorised leave for patients who present a significant risk to themselves or the public.
[13] Updated guidance will be issued in 2015. Until that point the Interim Guidance for Managing Screening Incidents (2013) should be followed.
[14] It is recognised that in some cases ward closure may be the safest/ most responsible action to take but in order to identify problems in service/care delivery , contributing factors and fundamental issues which need to be resolved an investigation must be undertaken
[15] For further information relating to emergency preparedness, resilience and response, visit: http://www.england.nhs.uk/ourwork/eprr/
[16] As an outcome loss in confidence/ prolonged media coverage is hard to predict. Often serious incidents of this nature will be identified and reported retrospectively and this does not automatically signify a failure to report.

2. Identification and immediate action

Serious incidents or suspected serious incidents must be declared internally as soon as the healthcare provider becomes aware of the incident. A senior manager or clinician should be identified by the health care provider's chief executive or equivalent, or the officer with relevant delegated authority, to undertake the following:

- Arrange for any immediate actions required to ensure the safety of the patient(s), other services users and staff.
- Obtain all relevant physical, scientific and documentary evidence, and make sure it is secure and preserved. Initial actions of local managers in the collection and retention of information are important for the overall integrity of the investigation process.[35]
- Identify witnesses, including staff, and other service users, to ensure they receive effective support.
- Identify an appropriate specialist/clinician[36] to conduct an initial incident review (characteristically termed the 72-hour review) to confirm whether a serious incident has occurred and if applicable, the level of investigation required and to outline immediate action taken (including where other organisations/partners have been informed)
- Ensure commissioners and other relevant parties (for example, police, Safeguarding Professionals, the Information Commissioner's Office) are informed at the earliest opportunity and within 2 working days of a serious incident being identified.
- Agree who will make the initial contact with those involved, or their family/carer(s). Where an individual(s) has been harmed by the actions of a patient, particular thought should be given to who is best placed to contact the victim and/or their family. Where necessary the provider must contact the police and agree with them who will make the initial contact with the victim(s), their family/carer(s) and/or the perpetrator's family. Those involved should have a single point of contact within the provider organisation.
- Arrange appropriate meeting(s) with key stakeholders, including patients/victims and their families/carers as required.
- Ensure the incident is appropriately logged on the serious incident management system STEIS (the Strategic Executive Information System, NHS England's web-based serious incident management system) or its successor system (see Part Three; section 3 below). Some incident types require additional reporting to other systems. See appendix 2 for further details.

As discussed in Part One of this guidance, it is often clear that a serious incident has occurred but where this is not the case providers should engage in open and honest discussions with their commissioners (and others as required) to agree the appropriate and proportionate response. Where it is not known whether or not an incident is a

[35] Advice from Information Governance leads should be sought early on to help support this process. They can advise on what information can/should be used and what needs to be done to support the use of personal and patient confidential information. Appropriate use of information that might relate to court or judicial proceedings should also be discussed and understood as appropriate.

[36] A clinician with relevant expertise who is not involved in delivery of care to the patient

serious incident, it is better to err on the side of caution and treat the incident as a serious incident until evidence is available to demonstrate otherwise. Serious incident reports can be downgraded and relevant records amended at any stage in the investigation[37]. Any downgrading must be agreed with the relevant commissioner on a case by case basis. Incidents that are found to not meet the threshold of a serious incident must be managed in line with the organisation's risk management and patient safety policies if appropriate.

3. Reporting a Serious Incident

Serious incidents must be reported by the provider to the commissioner without delay and no later than 2 working days after the incident is identified. Incidents falling into any of the serious incident categories listed below should be reported immediately to the relevant commissioning organisation upon identification. This should be done by telephone as well as electronically:

- Incidents which activate the NHS Trust or Commissioner Major Incident Plan:
- Incidents which will be of significant public concern:
- Incidents which will give rise to significant media interest or will be of significance to other agencies such as the police or other external agencies:

Out-of-hours, the local on-call management procedures must be followed.

Reporting a serious incident must be done by recording the incident on the NHS serious incident management system, STEIS,[38]or its successor system. The serious incident report must not contain any patient or staff names and the description should be clear and concise.

Other regulatory, statutory, advisory and professional bodies should be informed about serious incidents depending on the nature and circumstances of the incident. Serious incident reports must clearly state that relevant bodies have been informed. See Appendix 2 for a list of other organisations that must be considered. In some circumstances, where a serious incident or multiple serious incidents raise profound concerns about the quality of care being provided, organisations should consider calling a Risk Summit, which provides a mechanism for key stakeholders in the health economy to come together to collectively share and review information.[39]Most serious incidents will not warrant this level of response however.

All serious incidents which meet the definition for a patient safety incident should also be reported separately to the NRLS for national learning. Organisations with local risk

[37] This may depend on local procedures and capacity to ensure de-logging of incidents is performed in a timely manner.

[38] Providers require an N3 connection and authorisation from their local NHS England Area Team in order to set up a STEIS account. Where providers are unable to access STEIS the commissioner must report the serious incident on the system on the provider's behalf. A suitable Serious Incident Review Form (example provided in Appendix 6) should be completed in these circumstances in order to inform the relevant commissioner.

[39] Guidance available online at http://www.england.nhs.uk/ourwork/part-rel/nqb/