Requirement 320: Serious Incident reporting

Information security incidents are any event that has resulted or could have resulted in the disclosure of confidential information to an unauthorised individual, the integrity of the system or data put at risk or the availability of the information through the system being put at risk. Incidents may include theft, misuse or loss of equipment containing confidential information or other incidents that could lead to authorised access to data.

1. Procedures for Dealing with various types of Incident

Any suspicious incidents to the clinical governance and performance lead and managed in accordance with the Serious Incident Policy.

Incidents should always be investigated immediately whilst there is still the possibility of collecting as much evidence as possible. Investigations should normally be co-ordinated by the clinical governance and performance lead (or IG Lead if separate).

The following procedures should be followed for particular breaches:

A) Theft of equipment holding confidential information:

- If the cause is external inform the police and ask them to investigate
- If the cause is internal, establish the reason for the theft/ unauthorised access
- Consider the sensitivity of the data and the risk that it will be misused, to support assessing whether further action is appropriate
- Consider whether there is a future threat to system security and the need to take protective action e.g. change passwords
- Categorise and report the incident as described as per 'recording and reporting' requirements.

B) Access to patient records by an authorised user who has no work requirement to access the record:

- Interview the person reporting the incident to establish the cause for concern.
- Establish the facts by;
  - Asking the system supplier to conduct an audit on activities by the user concerned.
  - Interviewing the user concerned.

- Establish the reason for unauthorised access.
- Consider the sensitivity of the data and the risk to which the patient(s) have been exposed and consider whether the patient(s) should be informed.
- Take appropriate disciplinary action with directors and action with the patient(s) where appropriate.
- Categorise and report the incident as described as per 'recording and reporting' requirements.

C) Inadequate disposal of confidential material (paper, PC hard drive, disks/tapes):

- Investigate how the data came to become inappropriately disposed.
- Consider the sensitivity of the data and the risk to which the patient(s) have been exposed and consider whether the patient(s) should be informed.
- Take appropriate action to prevent further occurrences. (e.g. disciplinary, advice/training,)
- Take appropriate action with the patient(s) as appropriate
- Categorise and report the incident as described as per 'recording and reporting' requirements.

D) Procedure for dealing with complaints about patient confidentiality by a member of the public, patient or a subcontractor's staff:

- Interview the complainant to establish the reason for the complaint (Note, any complaint by a patient must be investigated and handled in accordance with the Complaints policy)
- Investigate according to the information given by the complainant and take appropriate action.
- Take appropriate action with the patient(s) as appropriate
- Categorise and report the incident as described as per 'recording and reporting' requirements.

E) Loss of data in transit e.g. when posting GOS 18 referral forms to the GP surgery or to the Hospital Eye Service.

- Investigate, as far as possible what has gone missing and where
- Consider the sensitivity of the data and the risk to which the patient(s) have been exposed and consider whether the patient(s) should be informed.
- Take appropriate action to prevent further occurrences. (e.g. process (was the envelope correctly addressed, is there further safeguards that could be introduced).
- Take appropriate action with the patient(s) as appropriate

- Ca
tegori
se

and report the incident as described as per 'recording and reporting' requirements

Serious Incidents Policy

The Company will respond to serious incidents in a timely, comprehensive and systematic manner in order to reassure concerned parties and improve future service. This Serious Incidents Policy has been developed in accordance with the NHS Serious Incident Framework March 2013.

The Company's policy incorporates full support for its subcontractors in ensuring they are part of the overall process, while seeking to avoid focus on particular individuals. Subcontractor practices must have in place and maintain staff suitably trained and competent in emergency preparedness, resilience and response. The Company's Incident Response Plan below demonstrates the process for subcontractor practices to notify the company in the event of a serious incident occurring.

The Company has incorporated transparency for all parties as a core theme in its serious incidents policy as the Company considers this is the only way to understand how serious incidents occur and how these can be mitigated in the future. The Company fully subscribes to the 'duty of candour' requirement in order to promote openness and honesty in raising early warning signs and demonstrate evidence of learning from incidents. The Company will ensure that patients are informed when things go wrong, why they have gone wrong and what steps the Company is taking to mitigate any issues, both immediately and in the future.

A mechanism for apology as part of duty of candour will also be implemented. The Company will notify the person concerned (and their GP where appropriate) when a *r*eportable Patient Safety Incident occurs or is suspected to have occurred involving moderate to severe harm.

As the prime contractor, the Company recognises its accountability to the commissioning body.

The Company's Serious Incident Policy becomes activated when its complaints policy is not adequate for managing a particular situation. A separate safeguarding policy exists for children and vulnerable adults.

Serious incidents may take the form of:

- Avoidable or unexpected death
- A never event
- A serious incident whereby the Company's ability to deliver the service is compromised
- Data loss
- Allegations of physical misconduct or harm.

The response to these events will vary depending on the particular issue (e.g. the serious incident grading chart below for the appropriate response). If there is a suggestion that a criminal offence has been committed, the Company will contact the police as soon as made aware of the incident.

The Company's clinical governance and performance lead will be responsible for patient safety, incident management and reporting to all appropriate bodies. The clinical governance and performance lead will also act as the accountable emergency officer. The Company will identify a deputy to the clinical governance and performance lead, who will provide cover and act as the accountable emergency officer in the event that the lead is unavailable for any reason. The Company will work collaboratively with other bodies in managing serious incidents. It will:

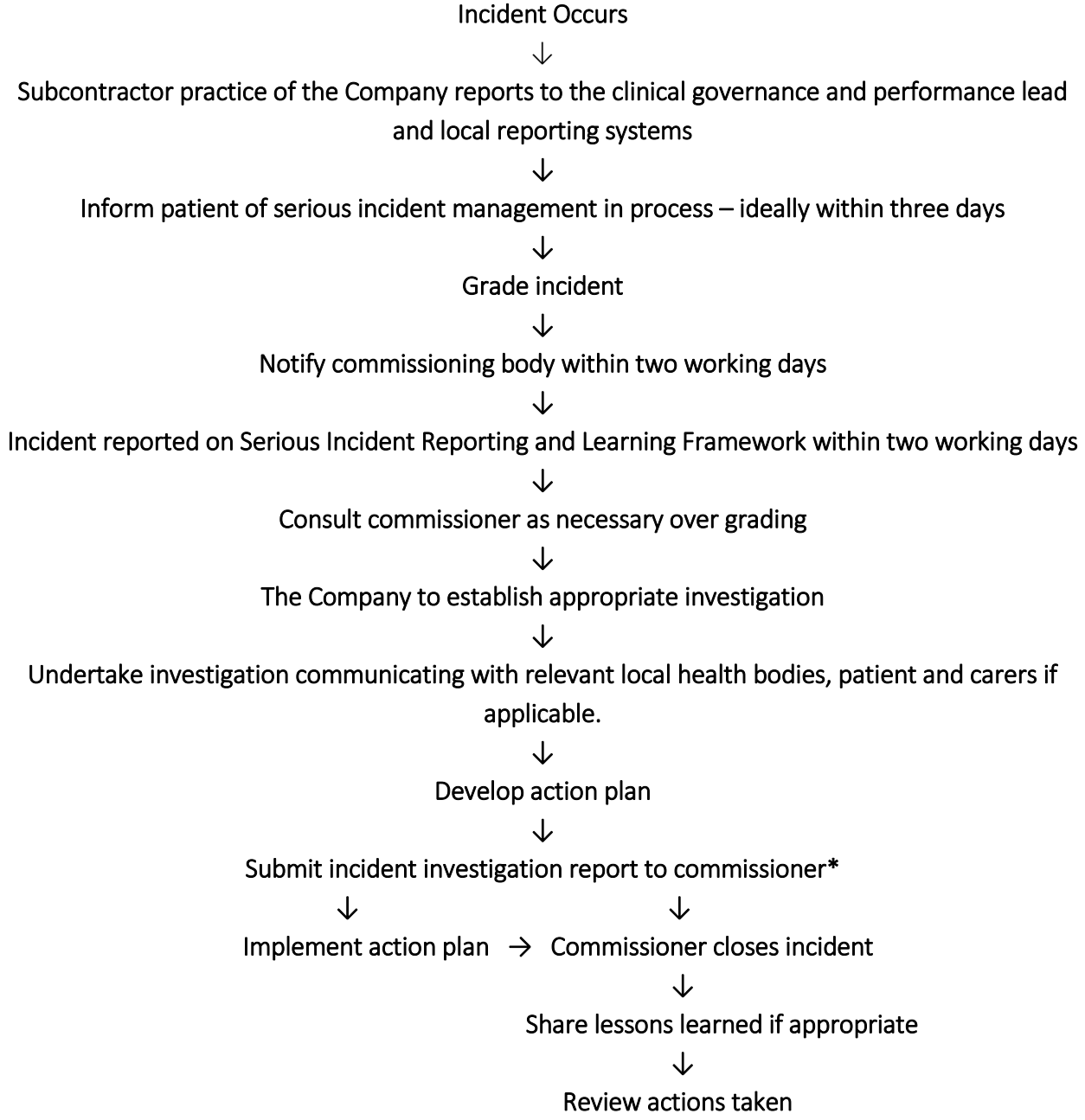
- Publish data (excluding information affecting patient confidentiality).
- Support and train staff in communicating information to patients.
- Communicate with commissioners and all relevant bodies as appropriate.
- Implement actions as required.
- Close cases in a timely manner.
- Review and analyse incidents and responses in order to learn key lessons and embed systemic improvements, in accordance with the Company's Quality and Continuous Improvement Policy.

The Company will implement a root cause analysis protocol as a methodical and systematic process to identify the specific factors that contributed to an incident. The Company's root cause analysis protocol seeks to understand the underlying causes and environmental context which led to a serious incident occurring, strengthening systems in place for meeting the objective of fully securing patient safety.

The Company's subcontractor practices do not have access to Strategic Executive Information System (STEIS). The Company will therefore build in reporting via the appropriate commissioning body for incident logging.

The Operations Centre of the Company's subcontractor, Webstar Health, will be the Incident Coordination Centre.

The Company operates the following serious Incident Response Plan for driving an appropriate learning experience to improve patient outcomes. This will enable the Company to ensure quality issues are raised in order to make improvements as required:



See below for the Company's grading/threshold charts of serious incident levels, their impacts/consequences and root cause analysis model we will use to continuously improve the overall quality of service.

Serious incident grading chart

Incident Grade	Example Incidents	Investigation Grade and action	Timeframe
1	Avoidable or unexpected death. Healthcare associated infections. Adult safeguarding incidents (see the Company's Safeguarding Policy for more information). Data loss and information security.	<u>Investigation Level 1:</u> Concise root cause analysis (RCA) for both No Harm and Low Harm and/or where the circumstances are very similar to other previous incidents. A concise RSA will enable the Company to ascertain whether unique factors exist, thus focusing resources on implementing service improvement. <u>Investigation Level 2:</u> Comprehensive RSA for incidents causing moderate to severe harm or death. The Company's policy is this will be the default investigation level for grade 1 incidents. Investigations will be carried out by directors of the Company and led by the clinical governance and performance lead who may seek advice and services from specialist external sources as required.	The Company to submit initial report within two working days. The Company will submit completed investigation within 45 working days.
2	Child protection incidents (see the Company's safeguarding policy for more information). 'Never events' Accusation of physical misconduct or harm. Data loss and information security (DH Criteria level 3-5).	Comprehensive RCA.	Initial report within 2 working days. The Company will submit a completed investigation within 60 working days.
	Selected grade 2 incidents These might include major systemic failure with multiple stakeholders.	<u>Investigation Level 3:</u> Independent RCA.	Initial report within 2 working days. Independent investigators should be commissioned to complete an investigation within 6 months

Root Cause Analysis Investigation Model

The Company will ensure it has sufficient expertise in root cause analysis. The clinical governance and performance lead will lead this process and report to the coordinating commissioner on progress and with the outcome. A model we will use is below:

	Action 1	Action 2	Action 3	Action 4	Action 5
Root CAUSE					
EFFECT on Patient					
Recommendation					
Action to Address Root Cause					
Level for Action (Org, Direct, Team)					
Implementation by:					
Target Date for Implementation					
Additional Resources Required (Time, money, other)					
Evidence of Progress and Completion					
Monitoring & Evaluation Arrangements					
Sign off - action completed date:					
Sign off by:					

This Serious Incidents Policy will be reviewed annually with commencement date 13/3/2017.