**[NAME] – “The Company”**

**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 2015 and Patient Safety Incident Response Framework (PSIRF) 2019.

The Company’s policy incorporates full support for its staff in ensuring they are part of the overall process, while seeking to avoid focus on particular individuals. The Company will ensure its staff are suitably trained and competent in emergency preparedness, resilience and response. The Company’s Incident Response Plan below demonstrates the process for responding to serious incidents.

The Company has incorporated transparency for all parties as a core theme in its Serious Incidents Policy as we consider this is the only way to understand how serious incidents occur and how they 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 areportable Patient Safety Incident occurs or is suspected to have occurred involving moderate to severe harm.

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 accountable emergency officer is [insert name] who is responsible for patient safety, incident management and reporting to all appropriate bodies. 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 does not have access to Strategic Executive Information System (STEIS). We will therefore build in reporting via the appropriate commissioning body for incident logging.

The Company operates the following 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:

Incident Response Plan

**Incident Occurs**

**↓**

**Company reports to local reporting systems**

**↓**

**Inform patient of serious incident management in process – ideally within three days**

**↓**

**Grade incident (grading chart below)**

**↓**

**Notify commissioning body within two working days**

**↓**

**Incident reported on Serious Incident Reporting and Learning Framework within two working days**

**↓**

**Consult commissioner as necessary over grading**

**↓**

**The Company to establish appropriate investigation**

**↓**

**Undertake investigation communicating with relevant local health bodies, patients and carers if applicable**

**↓**

**Develop action plan**

**↓**

**Submit incident investigation report to commissioner**

**↓ ↓**

**Implement action plan → Commissioner closes incident**

**↓**

**Share lessons learned if appropriate**

**↓**

**Review actions taken**

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. | **Investigation Level 1:**  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 RCA will enable the Company to ascertain whether unique factors exist, thus focusing resources on implementing service improvement.  **Investigation Level 2:**  Comprehensive RCA 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.  The Company 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 Companywill submit a completed investigation within 60 working days. |
| Selected grade 2 incidents  These might include major systemic failure with multiple stakeholders. | **Investigation Level 3:**  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 Company will manage this process and report to the 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 policy will be reviewed annually from [insert date].