Oxford University Hospitals
NHS Foundation Trust

Cover Sheet

Public Trust Board Meeting: Wednesday 15 January 2025

TB2025.11

Title:	**Emergency Preparedness Resilience and Response Core Standards Report 2024**

Status:	**For Information**
History:	**This is an annual report to Trust Board**

Board Lead:	**Chief Operating Officer**
Author:	**David Smith, Emergency Planning Officer**
Confidential:	**No**
Key Purpose:	**Assurance**

Executive Summary

1. This paper provides a report on the Trust's preparedness for emergencies.
2. NHS England published NHS core standards for Emergency Preparedness, Resilience and Response arrangements in 2024. These are the minimum standards which NHS organisations and providers of NHS funded care must meet. The Accountable Emergency Officer in each organisation is responsible for making sure these standards are met.
3. This paper provides a summary of the Trust's self-assessment of its preparedness against these standards. The Trust has been assessed as "Substantially Compliant" with the core standards.
4. This paper has been reviewed by Trust Management Executive.

Recommendations

5. The Trust Board is asked to note this report.

Emergency Preparedness Resilience and Response Core Standards Report 2024

1. Purpose

1.1. This paper provides a report on the annual audit of the Trust's emergency preparedness to meet the requirements of the Civil Contingencies Act (2004) and the NHS England Emergency Preparedness, Resilience and Response Framework (EPRR) 2022.

2. Background

2.1. NHS England published NHS core standards for Emergency Preparedness, Resilience and Response arrangements in 2024[1]. These are the minimum standards which NHS organisations and providers of NHS funded care must meet. The Accountable Emergency Officer in each organisation is responsible for making sure these standards are met.

2.2. This paper provides a summary of the Trust's self-assessment of its preparedness against these standards.

2.3. This year the annual assurance audit is separated into 2 parts for acute Trusts:

- Assessment against 62 core standards for EPRR
- A deep dive into 11 standards on cyber security

3. EPRR Core Standards

3.1. The outcome of this self-assessment shows that against 62 of the core standards which are applicable to the organisation, the Trust:

- is fully compliant with 61 of these core standards
- is partially complaint with 1 of the core standards
- is fully compliant against 11 deep dive standards

3.2. This gives an overall rating of "Substantially Compliant".

3.3. The Trust is partially compliant on standard 5. The Trust has an action plan in place to become fully compliant. This action plan is detailed below:

[1] https://www.england.nhs.uk/wp-content/uploads/2022/07/nhs-core-standards-for-eprr-2024-template-v2.xlsm

	Domain	Standard	Detail	Evidence - examples listed below	Organisation Evidence	Self assessment RAG.	Action to be taken	Lead	Timescale	Comments
5	Governance	EPRR Resource	The Board / Governing Body is satisfied that the organisation has sufficient and appropriate resource to ensure it can fully discharge its EPRR duties.	Evidence • EPRR Policy identifies resources required to fulfil EPRR function; policy has been signed off by the organisation's Board • Assessment of role / resources • Role description of EPRR Staff/ staff who undertake the EPRR responsibilities • Organisation structure chart • Internal Governance process chart including EPRR group		Partially compliant		Lisa Glynn	Quarter 4 (funding dependant)	The team consist of 1.5WTE which represents a single point of failure for the Trust. The ICS EPRR Lead will ask NHS England to review recommended minimum whole time equivalence levels. A business case is currently being considered to increase the establishment in the EPRR team from 1.5 wte to 2.0 wte.

3.4. Whilst the Trust is fully compliant on the 11 deep dive core standards it should be noted that the impact of a serious cyber-attack on the Trusts systems could likely severely impact on patient care. The recovery from a cyber-attack was not considered in the deep dive standards. Recovery from such an incident could take many weeks to months before systems were fully restored. The cyber-attack on Advanced Healthcare Ltd on 4 August 2022 caused Oxford Health FT to lose access to Carenotes, Adastra and finance and procurement systems. Full systems recovery was not completed until 12 December 2022.

4. Recommendations

4.1. The Trust Board is asked to note this report.