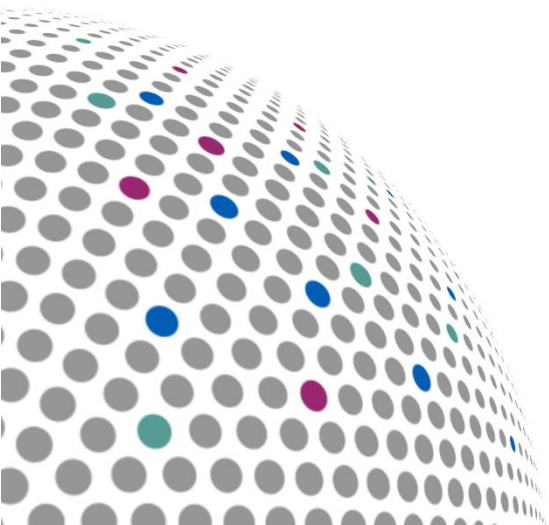
Data Security and Protection Toolkit Assurance 2018/19

Hull & East Yorkshire Hospitals NHS Trust



MIAA
IMPROVE THE OUTCOME

Introduction

There continues to be well publicised data breaches and service disruptions, including high-profile public sector data losses that have resulted in over one million pounds in monetary penalties being issued to NHS organisations by the Information Commissioner.

As of 2018 the IG toolkit was refreshed and replaced with the new Data Security and Protection Toolkit (DSPT). Whilst the standards have been updated it remains a tool which allows organisations to measure their compliance against law and central guidance and helps identify areas of partial or non-compliance. In addition, there is a contractual obligation for providers to complete the DSPT and they are subject to audit against it and must:-

- Inform the coordinating commissioner of the results of the audit; and,
- Publish the audit report both within the NHS Data Security and Protection Toolkit and on their website.

Objectives & Scope

The objective of the review was to provide an opinion on:

- The governance process, policies, and systems in place to complete, approve and submit the DPST Toolkit submisson;
- The validity of the assertions of the DPST submission based on the evidence available at time of audit for the reviewed sample; and,
- Any wider risk exposures and / or mitigations brought to light by review of that evidence.

Assurance Statement

The Trust has demonstrated that it has implemented an adequate Information Governance framework which is active. It has demonstrated evidence to confirm its assertion in the toolkit, or plans to reach compliance before final submission. However, further work has been identified as being required in regards to this work in relation to its assurances regarding the management of supplier contracts.

There is a good system of internal control designed to meet the system objectives, and that controls are generally being applied consistently.

Based upon the opinions on the following page, the overall assurance level provided in relation to information governance within the Trust, and within the limits of the scope described above is:-.

Substantial Assurance

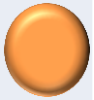
Basis of Assurance –

Area	Rating	Rationale
Governance		The Trust has demonstrated that has implemented a robust and active, framework to progress its Information Governance agenda. The Information Governance Committee meets quarterly and is chaired by the Trust's Data Protection Officer and Director of Corporate Affairs (Board Member). The Finance Director is the Trust's Senior Information Risk Owner (SIRO) and the Trust has recently appointed a new Caldicott Guardian, the Acting Medical Director. Throughout the year, the IG Framework has been supported by the IG Team with the appropriate skill sets.
Validity		We have been able to agree the validity all of the sample assertions reviewed at this point in the Trust's submission development. In particular, the Trust have made significant progress with regard to accountable suppliers that handle personal, identifiable data and the development of a comprehensive Information Asset Register. A detailed working action plan showing our assessments, any recommendations, risk ratings and responses by responsible officers have been shared under separate cover for the Trust to track progress prior to final submission.
Wider-Risk		As noted above, the Trust's supplier contract management and due diligence activities have been robust and this process needs to be rolled out to any new suppliers contracting with the Trust.

Assurance Definitions and Risk Classifications

Assurance Rating	Rationale
High	There is a strong system of internal control which has been effectively designed to meet the system objectives, and that controls are consistently applied in all areas reviewed.
Substantial	There is a good system of internal control designed to meet the system objectives, and that controls are generally being applied consistently.
Moderate	There is an adequate system of internal control, however, in some areas weaknesses in design and/or inconsistent application of controls puts the achievement of some aspects of the system objectives at risk.
Limited	There is a compromised system of internal control as weaknesses in the design and/or inconsistent application of controls puts the achievement of the system objectives at risk.
No	There is an inadequate system of internal control as weaknesses in control, and/or consistent non-compliance with controls could/has resulted in failure to achieve the system objectives.

Assurance Definitions and Risk Classifications

Risk Rating		Rationale
Critical		Control weakness that could have a significant impact upon, not only the system, function or process objectives but also the achievement of the organisation's objectives in relation to: • the efficient and effective use of resources • the safeguarding of assets • the preparation of reliable financial and operational information • compliance with laws and regulations.
High		Control weakness that has or is likely to have a significant impact upon the achievement of key system, function or process objectives. This weakness, whilst high impact for the system, function or process does not have a significant impact on the achievement of the overall organisation objectives.
Medium		Control weakness that: • has a low impact on the achievement of the key system, function or process objectives; • has exposed the system, function or process to a key risk, however the likelihood of this risk occurring is low.
Low		Control weakness that does not impact upon the achievement of key system, function or process objectives; however implementation of the recommendation would improve overall control.

One trusted business. Two different services

MiAA ASSURANCE

MiAA SOLUTIONS