

Data Security and Protection Toolkit Assurance 2019/20

Warrington and Halton Teaching Hospitals NHS
Foundation Trust

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 submission;
- The validity of the assertions of the DPST submission based on the evidence available at time of audit for the reviewed sample;
- The progress and completion of recommendations highlighted and detailed within the feedback spreadsheet for the 18/19 audit and reporting mechanisms for any actions highlighted on the Trust improvement plan if one was included as part of its 18/19 submission; 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 a robust 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. The Trust continue to populate the Information Asset Register and dataflow mapping solution which was initiated in 2018/19 and remains 'work in progress'. This remains fundamental to many requirements in the toolkit and therefore should continue to be progressed.

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		<p>Warrington and Halton Teaching Hospitals NHS Foundation Trust has demonstrated that it has implemented a robust, active framework to progress its information governance agenda. The Information Governance and Corporate Records Sub Committee (IGCRSC) meets bi-monthly and is chaired by the SIRO (Chief Information Officer) and is attended by the Caldicott Guardian (Acting Executive Medical Director/Chief Clinical Information Officer) and the Trust's Data Protection officer. Other key staff are co-opted onto the Sub-Committee as required e.g. Information Asset Owners. The IGCRSC reports into the Quality Assurance Committee which is a sub-committee of the Trust Board.</p>
Validity		<p>We have been able to agree the validity of the majority of the sample of assertions reviewed at this point in the Trust's submission development. The only area of concern was the Trust's current training percentage which currently falls below the mandated 95% target. However, senior management have been kept informed of progress and proactive measures are being taken in a bid to increase update especially across high risk staff groups.</p> <p>In addition, although the desktop exercise to test the Trust's ability to respond effectively to a data security incident had not been undertaken as yet, plans were well underway before the March submission deadline.</p> <p>A detailed feedback action plan detailing our assessments, recommendations, risk ratings and responses by responsible officers have been shared separately for the Trust to track progress prior to final submission.</p>
Follow-up		<p>The Trust has demonstrated progress in all the action points highlighted in the previous years report. However, work remains in progress to populate the new Information Asset Register and Data Flow Mapping solution.</p>
Wider-Risk		<p>As noted above, some areas remain work in progress at this point. In particular, assurance regards the completion of the Information Asset Register.</p>



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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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

