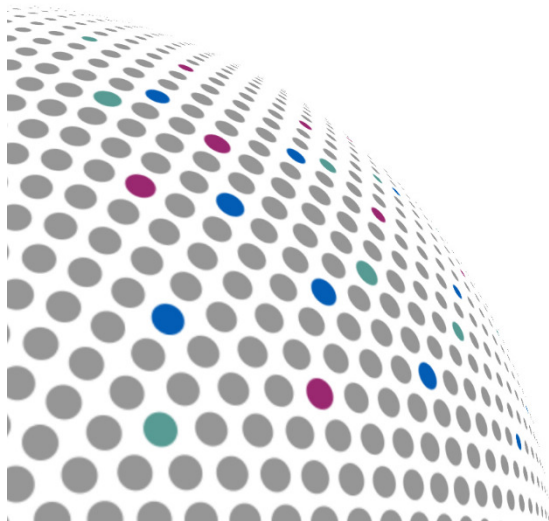


Data Security and Protection Toolkit Assurance 2018/19

The Walton Centre
NHS Foundation 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 submission;
- 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

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 –

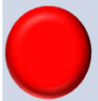



Area	Rating	Rationale
Governance		There is a clear organisational governance structure with associated processes and key roles in place, including the SIRO (Senior Information Risk Owner), Caldicott Guardian, Data Protection Officer and IG Manager / team. Structures/ committees appear to be operating, with action plans subject to oversight.
Validity		<p>4 DSP Toolkit requirements were sampled as part of the 2018/19 validation process. As of late Jan. 2019, there is a good system of internal control, and we have been able to agree the majority the Trusts assertions, in the remaining area the Trusts delivery plan for completion appears reasonable. There were some additional areas where we have provided recommendations for further consideration beyond the validity of the Toolkit submission.</p> <p>A detailed action feedback 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>
Wider-Risk		<p>As noted above, there are some areas highlighted by the work where recommendations have been raised for ongoing consideration. In particular the Trust should ensure completion of:</p> <ul style="list-style-type: none"> • Updated evidence for the contracts / suppliers work of the compliance mechanisms in place to provide assurance that the suppliers are complying with contracted data protection requirements and that the Trust has appropriate contracts in place, specifically for those assets the Trust has rated critical. • Confirmation of the accuracy and configuration of the reporting toolkit for the anti-virus figures as the current reporting appears low. <p>Other areas for consideration include:-</p> <ul style="list-style-type: none"> • Confirm implementation of planned framework / strategy / policy updates and publications, including the publication of the new DPIA register and formal publication of new / updated procedures and policy. • Confirm completion of additional reviews / updates to the information asset register for the Trust and provide evidence of report submission to Board sub-committee as planned for this reporting year. • Confirm implementation and provide evidence of ongoing activities, such as the completion of the ongoing system and Data Quality reviews as planned prior to submission. • Update evidence for timely statistics, including data breach reporting, and going forward, continue to develop compliance processes to ensure the ongoing evidencing of these timely requirements.



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

