



**AGENDA ITEM**

4.3

**DIGITAL & DATA COMMITTEE**

**ICO Audit Action Plan**

<b>Date of meeting</b>	13 March 2023	
<b>FOI Status</b>	Open/Public	
<b>If closed please indicate reason</b>	Not Applicable - Public Report	
<b>Prepared by</b>	Andrew Nelson, Chief Information Officer	
<b>Presented by</b>	Andrew Nelson, Chief Information Officer	
<b>Approving Executive Sponsor</b>	Stuart Morris, Director of Digital	
<b>Report purpose</b>	FOR NOTING	
<b>Engagement (internal/external) undertaken to date (including receipt/consideration at Committee/group)</b>		
<b>Committee/Group/Individuals</b>	<b>Date</b>	<b>Outcome</b>
N/A		

**ACRONYMS**

ICO – Information Commissioners Office

UHB – University Health Board

NCSC – National Cyber Security Centre

DPIA – Data Protection Impact Assessment

## **1. SITUATION/BACKGROUND**

- 1.1 The purpose of this report is to update the Committee on the UHB's progress in enacting the recommendations made by Officers of the Information Commissioner following their assurance visit in January 2022.

## **2. SPECIFIC MATTERS FOR CONSIDERATION BY THIS MEETING (ASSESSMENT)**

- 2.1 Further to their assessment in January 2022, Officers of the Information Commissioner made 35 recommendations regarding actions the UHB should be taking to reduce the UHB's risk of non-compliance with data protection legislation. A visit to review progress was made by the officers of the ICO in December 2022 at which they identified that they required a higher threshold of evidence to be available than the UHB had offered.
- 2.2 Throughout 2022 the UHB has continued to take a risk-based approach to all areas of its operations. The focus around data protection has largely been on cyber security, acting on advice of the NCSC and the Cyber Resilience Unit and in ensuring that DPIAs, data sharing agreements and cyber security impact assessments have been undertaken for all new activities or changes in activities. A more detailed description of the cyber actions is provided in the confidential paper the UHB's cyber improvement plan, whilst an update on the progress made in delivering the ICO's recommendations is provided in the Excel document attached.
- 2.3 As a consequence, a subjective assessment by the Information Governance (IG) team, would suggest that the UHB has made minimal progress against 15 of the recommendations, and partial progress against a further 12.
- 2.4 The most significant constraint to improvement remains the staffing position in both IG and cyber security. Based on current resource allocation decisions taken by the Board, these will deteriorate in the next few weeks as resources do not permit the extension of the contractor arrangements for a Head of Information Governance at premium rates to continue beyond 31<sup>st</sup> March 2023, nor for the IG administrator post to be replaced, following the postholders acceptance onto a national training programme.
- 2.5 A further follow up meeting with the officers of the ICO is planned for the last week of March 2023.

## **3. KEY RISKS/MATTERS FOR ESCALATION TO BOARD/COMMITTEE**

- 3.1 The Committee is requested to note the progress attached in Appendix 1.



3.2 14 of the recommendations which remain outstanding have been prioritised as High by the ICO. Whilst there is a degree of understanding by the ICO’s officers of the challenges that the UHB is facing, it is possible that the result of the March review will not only extend the length of the ICO’s engagement with the UHB but may lead to a more directive report and the ICO wishing to increase the awareness of members of our population and those we share data with, of the shortcomings in our controls and procedures.

#### 4. IMPACT ASSESSMENT

<b>Quality/Safety/Patient Experience implications</b>	Yes (Please see detail below)
	Ransomware attack has demonstrated significant impact on patient care and staff welfare.
<b>Related Health and Care standard(s)</b>	Governance, Leadership and Accountability
<b>Equality Impact Assessment (EIA) completed - Please note EIAs are required for <u>all</u> new, changed or withdrawn policies and services.</b>	No (Include further detail below)
	Equality Impact Assessment to be completed as part of each project
<b>Legal implications / impact</b>	Yes (Include further detail below)
	UHB non compliance with GDPR & NIS-D.
<b>Resource (Capital/Revenue £/Workforce) implications / Impact</b>	Yes (Include further detail below)
	Potential fine for non compliance with GDPR & NIS-D.
<b>Link to Strategic Goals</b>	Improving Care

#### 5. RECOMMENDATION

5.1 The Committee is asked to **NOTE** the report and to consider whether the progress made in delivering the data protection improvement programme and the continuing focus of the IG resource on cyber security and new

data sharing arrangements is appropriate and in line with the Board's Assurance Framework.

5.2 To **NOTE** the potential outcome of the ICO review in March 2023