NHS Nottingham West Clinical Commissioning Group

NHS Nottingham North and East Clinical Commissioning Group

NHS Rushcliffe Clinical Commissioning Group

NHS Mansfield and Ashfield Clinical Commissioning Group

NHS Newark and Sherwood Clinical Commissioning Group

Information Governance, Management & Technology (IGMT) Committee Highlight Report

23 March 2018

Information Governance, Management and Technology Committee Annual Report 2017/18.
The Committee **APPROVED** the Annual Report for 2017/18. The annual report provided an overview of the activities and achievements of the IGMT Committee throughout 2017/18 and its objectives for 2018/19. The IGMT Committee was established on behalf of NHS Rushcliffe (RCCG), NHS Nottingham North and East (NNE), NHS Nottingham West (NW), NHS Mansfield and Ashfield (M&A) and NHS Newark and Sherwood (N&S). The purpose of the Committee was to support and drive the broader information governance (IG) and information management & technology (IM&T) agendas.

Data Quality Policy.
The Committee **APPROVED** the Data Quality Policy. The purpose of the policy was to set out a clear policy framework for maintaining and increasing high levels of data quality within the CCGs. The way in which data was collected and analysed could influence the results and it was, therefore, important to have a clear and open framework in place which supported this process and accurately reflected the practice of the CCGs in the discharge of their functions. The Data Quality Policy set out how the CCGs would collect, analyse and report data. Amendments to the previous version included references to the General Data Protection Regulation.

Access to Patient or Staff Information by Using a Smart Card Policy.
The Committee **APPROVED** the Smart Card Policy. This policy was intended to provide clear guidance on the roles and responsibilities for users of HSCIC Applications. Accessing personal confidential data would be through the process of issuing a Smartcard and a Personal Identification Number (PIN). The policy had been reviewed by IG Leads, who had provided advice regarding the information governance elements and DP and Registration Authority (RA) managers at NHIS had reviewed from a technical. The policy had also been updated to reflect changes to NHS Digital and IG toolkit changes.

EU General Data Protection Regulation Update.
The Committee **NOTED** an update on the EU General Data Protection Regulation (GDPR). The General Data Protection Regulation (GDPR), was approved in 2016 and would come into force on 25 May 2018. There was greater focus on evidence-based compliance with specified requirements for transparency, more extensive rights for data subjects and considerably harsher penalties for non-compliance. The GDPR introduced a principle of 'accountability' that required organisations must be able to demonstrate compliance. The purpose of the document presented was to provide an update on the national and local position for GDPR. It described the changes being introduced by the new legislation and how the Nottinghamshire CCGs were addressing the requirements.

Update on governance structures and impact on Committee.
The Committee **NOTED** an update on CCG governance structures. The Greater Nottingham CCGs were aligning their management structure and agreeing a shared committee structure. Delegated authority from South Nottinghamshire CCG Governing Bodies would likely be removed from the Committee as a result of changes, however, it was anticipated that the work of the Committee would still continue as an operational group. The terms of reference for the Committee would be reviewed and presented at the following meeting for agreement, to include changes to membership and links with governance structures for Greater Nottingham CCGs and Mid Nottinghamshire CCGs.

Lessons Learned from the WannaCry ransomware cyber-attack.
The Committee **NOTED** the Lessons Learned from the WannaCry ransomware cyber-attack report and associated action plan. The Department of Health and Social Care had commissioned a review of May 2017's WannaCry ransomware attack. The purpose of the report was to analyse the lessons learned, assess actions taken so far and make clear recommendations on what further measures were required to ensure the health and social care system was as robust as it could be. The report set out a number of recommendations to strengthen the resilience and ability of local organisations to respond to the increasing cyber threat. NHIS had reviewed the recommendations and proposed that where these should be actioned by local organisations, the partners should use the Cyber Security Assurance Programme to embed these and monitor progress against the recommendations.

IG Toolkit updates.
The Committee **NOTED** an update on the IG Toolkit audits. 360 Assurance had conducted the annual IG toolkit audit during January and February 2018 and final reports were awaited. South Nottinghamshire CCGs would meet all the requirements for the IG toolkit for submission in March 2018 and would submit compliance at 67%, level 3 for indicator 130 and level 2 for all other indicators. Mid Nottinghamshire CCGs would meet all the requirements for the IG toolkit submission in March 2018 and would submit compliance at 80% with 11 indicators at level 3 and 16 indicators at level 2.

Information Governance Risk Register and Issues Log.
The Committee **DISCUSSED** the information governance risk register and issues log. The Committee discussed the risk description and score for the cyber security risk. It was agreed that the risk description required rewording to reflect a loss of systems, rather than a risk to confidentiality and security with scoring amended to reflect this with an initial likelihood score of 5 and an impact score of 5 and a residual risk scoring of likelihood score of 5 and an impact of 4. This would escalate the risk for most CCGs to their Assurance Frameworks for monitoring and oversight by Governing Bodies and Audit Committees.