Clinical Commissioning Group (CCG) Governing Body 2019/2020 – Part 1

Date of Meeting:	17 January 2020
Agenda Item:	4.4
Subject:	IGMG and Cyber Security Update
Reporting Officer:	Sam Evans
Aim of Paper:	To provide a quarterly update on IG and Cyber Security

Governance route prior to Governing Body	**Meeting Date**	**Objective/Outcome**
Governing Body	Select date of meeting.	Click to Select
Audit Committee	Select date of meeting.	Click to Select
Corporate Governance Committee	Select date of meeting.	Click to Select
Strategic Place Board	Select date of meeting.	Click to Select
Integrated Commissioning Board	Select date of meeting.	Click to Select
Locality Engagement Group	Select date of meeting.	Click to Select
Patient and Public Engagement Committee	Select date of meeting.	Click to Select
Quality and Safeguarding Committee	Select date of meeting.	Click to Select
Remuneration Committee	Select date of meeting.	Click to Select
Clinical and Professional Advisory Panel	Select date of meeting.	Click to Select
Primary Care Commissioning Committee	Select date of meeting.	Click to Select
Other	Information Governance Management Group	

Governing Body Resolution Required:	For Information Only
Recommendation	To note the contents of the paper

Link to Strategic Objectives		**Contributes to:** (Select Yes or No)
SO1:	To be a high performing CCG, deliver our statutory duties and use our available resources innovatively to deliver the best outcomes for our population.	Yes
SO2:	To deliver on the outcomes of the Locality Plan in respect of **Prevention and Access** (Prevention and Self Care)	No
SO3:	To deliver on the outcomes of the Locality Plan in respect of **Neighbourhoods & Primary Care** (Getting help in the Community)	No
SO4:	To deliver on the outcomes of the Locality Plan in respect of **In Hospital - Planned** (Getting more help)	No
SO5:	To deliver on the outcomes of the Locality Plan in respect of **In Hospital - Urgent Care** (Getting more help)	No
SO6:	To deliver on the outcomes of the Locality Plan in respect of **Children, young people and families**	No
SO7:	To deliver on the outcomes of the Locality Plan in respect of **Mental Health**	No

Risk Level: (To be reviewed in line with Risk Policy)	Green
Comments (Document should detail how the risk will be mitigated)	Sufficient controls and mitigating actions are in place to keep the risk level at green

Content Approval/Sign Off:	
The contents of this paper have been reviewed and approved by:	Chief Finance Officer, Health and Social Care Integration Sam Evans
Clinical Content signed off by:	Not applicable
Financial content signed off by:	Not Applicable

	Completed:
Clinical Engagement taken place	Not Applicable
Patient and Public Involvement	Not Applicable
Patient Data Impact Assessment	Not Applicable
Equality Analysis / Human Rights Assessment completed	Not Applicable

Executive Summary

This report updates Governing Body on the CCG Information Governance & Cyber Security position for the period ending 31st December 2019.

Information Governance

The CCG submitted its baseline assessment for the Data Security and Protection Toolkit (DSPT) in October 2019 to meet the national deadline for submission.

The CCG is on course to meet the final assessment for the end of March 2020 with:

- 76 of 106 mandatory evidence items provided
- 29 of 43 assertions confirmed

The CCG Assurance Team are in the process of working with GMSS and other providers to collect the remaining evidence items.

IG Training

- **DPO** - The CCG Data Protection Officer attended DPO training with the CCG Head of IT & Assurance in June 2019.

- **SIRO** The CCG SIRO and Deputy SIRO both attended annual SIRO training in December 2019.

- **Mandatory** - As of the last Information Governance Management Group meeting in December, IG training stats sit at 73% of employees are compliant with the target being 95%. The CCG Senior IG Lead will be following up compliance early in January to ensure non-compliant staff carry out their mandatory IG training.

Cyber Security

From the period of April -December 2019, there have been no Cyber Security incidents reported

- **Desktop Lockdown**

The NHS England GP IT Services Operating Model mandates that the CCG (via GMSS and IT Provider) must provide secure, well-managed and locked down workstations to GP Practices. Early in 2019, a policy was implemented to remove local administrator rights from the user accounts of all staff in GP surgeries and CCG's across Greater Manchester. This was a security measure that provides everyone on the GM Network with increased protection against malware attacks.

USB lockdown has also occurred during this period. Unauthorised USB Storage devices are now unable to be used on CCG devices unless a call is logged with GMSS (via the Head of IT & Assurance) and that device is whitelisted. All USB storage devices must be encrypted to AES 256 encryption.

- **CareCERT**

NHS Digital provides cyber security threat notifications to organisations where malicious activity has been detected through the Advanced Network Monitoring (ANM) solution applied at the HSCN and N3/TN internet gateways. Whilst it monitors all traffic passing through the gateway and blocks malicious traffic as it is detected, organisations may still have malware or other infections within their infrastructure. If organisations have their own Internet connectivity, this malicious traffic could still reach its intended destination. It is therefore essential that when notifications are received by organisations where malicious activity has been detected, that these notifications are acted upon to prevent any data loss or other unwanted behaviour.

GMSS monitor CareCERT alerts on behalf of supported CCG's and act upon them. The CCG Head of IT also receives these alerts directly. GMSS report on these alerts (notifications and resolutions) monthly at the GM IT Ops & Security Group.

In the period from April - December 2019 there have been no threat alerts for HMR CCG or GP Practices.

- **Internet Monitoring**

LogRythm was implemented in September 2019 to provide detailed analysis of internet traffic across the GM Network. It currently filters URL and reports on any inappropriate network traffic and streaming (from sites such as Spotify). Any such traffic is blocked from the network.

- **Domain Account Management**

GMSS monitor the domain for suspicious user behaviour that could be a sign of malware, virus or hacking activity. GMSS IT Security currently investigate all accounts that have over failed logon attempts to ensure nothing is amiss.

Recommendation

Members are asked to note the content of this report.