Barnet, Enfield and Haringey **NHS**

Mental Health NHS Trust

A University Teaching Trust

Title:	Information Governance Annual Report
Report to:	Trust Board
Date:	27 March 2017
Security Classification:	Public Board Meeting
Purpose of Report: This report provides an update in relation to Information Governance processes and procedures within the Trust. The report focuses on: • Information Governance Toolkit version 14 • Level 2 Information Governance incidents • New General Data Protection Regulation (GDPR)	
Recommendations: The Trust Board is asked to: 1. Note the contents of this report. 2. Endorse the action management plans in this report.	
Report Sponsor:	John Davidson, Chief Information Officer / Senior Information Risk Owner (SIRO)
Comments / views of the Report Sponsor:	This report is intended to assure the Board of the Trust's compliance with Information Governance requirements, including the submission of the internally audited 2016/17 Information Governance Toolkit. The Trust has exceeded the mandatory 'Level 2' on a number of Information Governance requirements and has achieved an overall score of 81% compared to last year's 78%.
Report Author:	Name: Doreen Todd Title: Information Governance Manager Tel Number: 020 8702 4134 E-mail: Doreen.todd@beh-mht.nhs.uk
Report History:	Third annual report to the Trust Board.
Budgetary, Financial / Resource Implications:	None

Equality and Diversity Implications:	NA
Links to the Trust's Objectives, Board Assurance Framework and / or Corporate Risk Register	Information governance is an essential part of the Trust meeting its registration standards.
Appendices: None.	

Report

1.   Introduction and Background

1.1   This report provides a briefing in relation to Information Governance and the Information Governance Toolkit (IGTK) version 14.

1.2   The NHS IGTK is a self-assessment strategic framework consisting of a range of linked initiatives (standards) that all NHS organisations are required to complete and submit to NHS Digital on an annual basis. The toolkit evaluates the adequacy of risk management and control within the Trust and assesses progress against these initiatives.

1.3   The IGTK only has two levels:
- Level 1 = not satisfactory
- Level 2 = satisfactory

1.4   Trusts need to reach a minimum of level 2 on each of the individual standards to attain an overall 'satisfactory' rating, failure to do so would impact on service delivery.

1.5   In accordance with the requirements of the IGTK, the purpose of this report is to provide the Board with assurances in relation to IG management and accountability, advise of any serious IG incidents and to provide an update in respect of the IGTK assessment. The report is produced prior to final submission of the IGTK reporting deadline listed below.

2.   IG Toolkit Version 14

2.1   IGTK formal reporting deadlines:
- Baseline assessment   due 31/07/16 - complete
- Performance Update   due 31/10/16 - complete
- Final submission   due 14/03/17 - complete

2.2   The Trust commissioned RSM LLP to undertake the annual internal audit which took place during the week commencing 5 December 2016.

2.3   Ten individual standards were randomly selected to be audited from the following categories:
- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance

2.4   The audit confirmed that the Trust's procedures for managing IG Toolkit improvement plans, including monitoring, reporting, and compliance was found to be sound.

2.5   An action plan to close any gaps identified at audit was agreed with the individual 'standard owners' and at the information governance group meeting.

2.6   A debrief meeting was arranged for week commencing 27/02/17, where the auditor confirmed that all necessary actions had been taken and that the evidence matched the criteria for the audit, and that there are no further outstanding actions.

2.7   The table below provides an overview of the previous years and the most recent IG toolkit submissions showing a steady improvement.

2011/12	70%	Satisfactory
2012/13	69%	Satisfactory
2013/14	70%	Satisfactory
2014/15	77%	Satisfactory
2015/16	78%	Satisfactory
2016/17	**81%**	**Satisfactory**

3.   Benchmarking

3.1   The table below shows how neighbouring Trusts compared for the previous years' IG Toolkit submission.

Trust	Score
Camden & Islington NHS Foundation Trust	91%
South London & Maudsley NHS Foundation Trust	89%
Surrey & Boarders Partnership NHS Foundation Trust	88%
Oxleas NHS Foundation Trust	87%
Central & North West London NHS Foundation Trust	86%
Tavistock & Portman NHS Foundation Trust	83%
Hertfordshire Partnership NHS Foundation Trust	81%
Barnet, Enfield & Haringey NHS Mental Health Trust	78%
West London Mental Health NHS Trust	77%
South West London & St Georges Mental Health NHS Trust	75%
East London NHS Foundation Trust	74%
North East London NHS Foundation Trust	70%

3.2   It is noted that all of the trusts who have declared a higher score than ours are Foundation Trusts. From recent benchmarking studies of IT spending, the cost of IG in our trust is amongst the lowest.

4.   2016/17 Improvement Plan

4.1   The Trust is dedicated toward continual improvement in accordance with the IG Toolkit/National legislation. It is acknowledged that new Data Protection legislation (detailed below) which includes stronger information rights, will bring challenges to organisations processing personal data. Upon the advice of the Information Commissioner the Trust has developed an action plan which is updated as new information/guidance is released.

5.   New General Data Protection Legislation (GDPR) – update

5.1   The General Data Protection Regulation (GDPR) will apply in the UK from 25 May 2018 and is currently being phased in as new guidance is made available.   The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

5.2   The primary objectives of the GDPR are to give individuals control of their personal data and to simplify the regulations for international organisations by unifying the regulation within the EU.

5.3   The Information Commissioner's website continues to provide updates as new information is released.

5.4   It is widely acknowledged that implementing the GDPR is likely to have significant resource implications, especially for larger and complex organisations. The Article 29 Working Party has indicated that there are considerable changes ahead. The Information Governance Alliance, whose aim is to become the authoritative source of advice and guidance in relation to GDPR information, will be writing to CEOs in April 2017 regarding the adoption and impact of the GDPR.

6.   Information Governance Incidents

6.1   Incidents are categorised as:
* Level 1 = Less serious Information Governance incidents
* Level 2 = Serious Information Governance incidents

Level 2 incidents must be reported to the Information Commissioners Office.

6.2   The table below provides an overview and comparison of Information governance incidents (excluding March 2017 – information not available at the time of writing this report)

Incident Description	2015/16	2016/17
Corruption or inability to recover electronic data	0	0
Disclosed in error	65	51
Lost in transit	0	0
Lost/stolen hardware	6	7
Lost/stolen paperwork	13	12
Uploaded to website in error	1	0
Technical security failing (including hacking)	0	0
Unauthorised access/disclosure	0	9
Other miscellaneous	13	20
Total incidents	**98**	**99**

Level 2 incidents	2	1

Incidents "Disclosed in error" and "Unauthorised access" include incidents where staff have disclosed person identifiable information when contacting the HP service desk or have shared passwords.

6.3   **Level 2 Incident:** This concerned a member of staff emailing confidential data to multiple recipients working on behalf of a local authority. The sender had emailed the data to a generic email inbox rather than a specific individual; in addition the sender had not used NHSmail (encrypted email) to transfer the data, as per Trust policy. The incident was reported to the Information Commissioners Office (ICO). Following investigation by the ICO Enforcement Team, the Trust were advised that no further action would be necessary at that time as appropriate remedial action had been taken to safeguard the data and manage the incident.

6.4   Actions taken to mitigate further incidents of a similar nature consist of:
* Raising staff awareness in relation to the use of NHSmail when sending confidential data outside of the organisation.
* Reviewing policies to ensure they were sufficiently robust

7.   Clinical Coding

7.1   Audit of clinical coded information is essential if the information created is to be accurate, complete, consistent and meaningful to the many legitimate users. The coding audit is pivotal for identifying clinical coding issues and evaluate information processes involved in

the collection of the data for clinical coding purposes, thereby ensuring continual improvements in the quality of the information produced. Accordingly, the Trust commissioned the annual clinical coding audit which took place week commencing 24/10/16. The result from the audit confirmed that the Trust had once again achieved level three. Level three has been sustained for the last three years primarily due to allocating the task to a professional clinical coder.

7.2   The table below provides details of the 2016/17 clinical coding audit.

Area	Level 2	Level 3	Trust % correct
Primary Diagnosis	>=85%	>=90%	**98.00% Level 3**
Secondary Diagnosis	>=75%	>=80%	**96.88% Level 3**

8.   Information Governance Training

8.1   Information Governance knowledge and awareness should be at the core of an organisation's objectives, embedded alongside other governance initiatives providing a stable foundation for the workforce. Without this knowledge, the ability of the Trust to meet its legal and policy requirements will be severely impaired.

8.2   The IGTK mandates that at least 95% of all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation have completed their annual IG training in the period 1 April to 31 March. The table below shows compliance recorded on 14/03/17.

Division	Staff count	Compliant	% achieved
Barnet	444	424	96%
Corporate	265	258	97%
Enfield	1203	1141	95%
Estates & Facilities	79	78	99%
Haringey	341	318	93%
Specialist services	687	630	92%
TOTAL	**3019**	**2849**	**94%**

9.   Budgetary / Financial Implications

9.1   Currently none, however additional resources will likely to be required to prepare to meet the needs of the new General Data Protection Regulation.

10.   Risk Management

10.1   Work is on-going to:
- Continue to raise information security awareness by means of staff communication / spot checks/line management cascade
- Progress with the NHSmail 2 project plan, which is planning to replace the Trusts unsecure email by June 2017, will reduce the likelihood of sending data via unsecure channels
- Continue to promote Information Governance via mandatory training.
- Monitor any updates regarding the new data protection legislation as and when available

11.   Equality and Diversity Implications

11.1   None.