Paper: 15

Date	Tuesday, 27 March 2018

Title of paper	**EU General Data Protection Regulation (GDPR) Compliance**

Presenter	Bill Sturman (Director of Informatics)				
Author	Bill Sturman (Director of Informatics)				
Responsible Director	Diane Jones (Director of Quality & Safety, BHH CCGs) Ben Westmancott (Director of Compliance, CWHHE CCGs) Bill Sturman – (Director of Informatics, NWL CCGs)				
Clinical Lead	Laurie Slater (Clinical IG Lead, CWHHE CCGs)				
Confidential	**Yes**	☐	**No**	☑	Items are only confidential if it is in the public interest for them to be so

The Governing Body is asked to:

Note the progress already made on ensuring NWL compliance with GDPR which comes into effect on the 25th May 2018 and the further plans to achieve compliance.

To approve the appointment of a 'Data Protection Officer' (a statutory requirement) and to approve the NWL CCG IG Committee as the governance vehicle to assure and achieve GDPR compliance. To note that, in the interim, the BHH IG Manager is supporting data protection officer duties.

Summary of purpose and scope of report

The General Data Protection Regulation (GDPR) comes into effect on the 25th May 2018. Not only do organisations have to comply with the GDPR, they also have to be able to demonstrate compliance. GDPR builds upon current Data Protection legislation rather than replacing it and increases fines up to 4% of the annual turnover of an organisation or up to 20million euros/£17million. Significant changes include strengthened data subject rights, breach reporting, documents required for accountability, consent, data protection by design and 'Data Protection Officers'.

NWL CCGs have instigated seven workstreams to achieve GDPR compliance comprising:

1. Pan-NWL Information Governance through the set-up of an IG committee. This will be the place where detailed compliance matters will be reviewed and action plans monitored
2. Appointment of a Data Protection Officer. In the interim the BHH IG Manager (Ernest Norman-Williams) is supporting DPO activities.
3. Ensure NWL Information Sharing Agreements are GDPR compliant
4. Educate and train GPs in the implications of GDPR including new 'Fair Processing

Notices'

5. Information security review in relation to the security of personal data and the security of information processing
6. Contracts review (clauses around data controllers/processors/sub-processors need to be transparent and compliant)
7. Ensure internal CCG departments which hold personal data are GDPR compliant. This includes documenting the purposes of holding data, records of processing activities and breach reporting.

Senior Information Risk Officers (SIROs) have been appointed for each workstream with progress and plans in place to achieve compliance by 25th May 2018.

The main risk to achieving GDPR compliance is the appointment of a permanent Data Protection Officer who can provide advice and guidance, and ultimately assure NWL GDPR compliance in May 2018 and beyond. This relates in particular to assuring compliance of internal CCG departments and contracts but covers all areas. In the event that NWL CCGs is not able to demonstrate compliance with GDPR by 25th May 2018, it is possible that the ICO may impose a fine. However this likelihood needs to be contextualised within a national context where every organisation needs to be compliant by the 25th May and also the challenging timescales for amendments to UK regulations.

Quality & Safety/ Patient Engagement/ Impact on patient services:

The GDPR will impinge on how we engage with patients either as Data controllers or as Data Processors. The legal basis for processing personal data is more robust giving more rights and control to the data subjects. For example, the legal definition of consent (Article 4 (11)) of the GDPR states that consent of the data subject means:

"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Records will need to be kept for consent to be verifiable –Article 7(1))

At a minimum 'Fair Processing Notices' in GP surgeries will need to transparently explain the use of patient data.

Finance, resources and QIPP

List implications for the organisation in terms of:

- Finance - Public Authorities are required to appoint a Data Protection Officer (DPO), there will also be need for financial investment in staff training and secure IT infrastructure.

- Staffing – A DPO covering NWL CCGs and primary care (the latter subject to capacity).

Equality / Human Rights / Privacy impact analysis
GDPR promotes “Privacy by design”, which requires that we carry out risk assessments, (Data Protection Impact Assessments-DPIA) to ensure we mitigate the risks identified before any change processes or projects are carried out by the organisation

Risk	**Mitigating actions**
Insufficient time to complete all activities and to be fully GDPR compliant in May 2018	Identification of workstreams and initiation of work. Appointment of DPO and governance structure to assure GDPR compliance
What CWHHE Corporate Objectives does it support and how?	Objective 6
What risks on the Board Assurance Framework or local CCG risk register does it impact upon or mitigate and how?	BAF entry 6.5

Supporting documents
Attached

Governance and reporting

(list committees, groups, other bodies in your CCG or other CCGs that have discussed the paper)

Committee name	Date discussed	Outcome
CWHHE / BHH SMTs	Jan - March 2018	Supported
Collaboration Board :BI and Informatics	01/03/2018	Endorsed
CCG Governing Bodies	March 2018	
NWL IG Committee	26/03/2018	Final Approval expected

Paper: 15

EU General Data Protection Regulation (GDPR) Compliance

1. Overview

The General Data Protection Regulation (GDPR) comes into effect on the 25th May 2018 . Not only do organisations have to comply with the GDPR, they also have to be able to demonstrate compliance. GDPR builds upon current Data Protection legislation rather than replacing it and increases fines up to 4% of the annual turnover of an organisation or up to 20million euros/£17million.

The substantive changes which GDPR brings are:

a) Strengthening Data Subject Rights including new rights about portability and the rights to object (e.g. the rights to have data "forgotten" (erasure), rectified and blocked (restricted) which must be much easier to use, stronger rights in relation to automated processing (including profiling), right of access (subject access requests) will be free and faster., stronger right to compensation).
b) Accountability breach reporting (any personal data breach must be reported directly to the Information Commissioner's office within 72 hours at the latest (currently it is not an obligation), personal data breaches must be documented (currently not an obligation)).
c) Data Protection Officer. This is a new **statutory** role required for public authorities and large scale processers. Defined as the cornerstone of compliance (informs and advises on compliance, monitors compliance including training, awareness raising, audits and assignment of responsibilities, the first point of contact for ICO, independent expert and directly reports to the highest level within organisation).
d) Documents required to underpin accountability. Some are expressly required under GDPR including a record of processing (limited exemption), records of consent, controller-processor contracts, Data Protection Impact Assessments, records of personal data breaches. Other documents are implicated under accountability requirement e.g. policies, DPO documents.
e) Stricter conditions for consent (must be freely given, specific, informed and unambiguous, consent must be as easily revoked as given, specific rules will apply to children in relation to information society services).
f) Data Protection by design (privacy by design and the default behaviour). Organisations must implement technical and organisational measures to show that they have considered and integrated data compliance measures into our data processing activities. Data Protection Impact Assessments are now required (was best practice) where there is a high risk to the rights and freedoms of individual, particularly for new technologies.

Further detail on the GDPR changes to the DP Act may be found at https://www.eugdpr.org/ .

Paper: 15


CWHHE
Central London.
West London.
Hammersmith & Fulham.
Hounslow.
Ealing.
Clinical Commissioning Groups

Paper: 15

2. Areas of work for NWL CCGs and SIROs (Senior Information Risk Owner)

In order to comply with GDPR, NWL CCGs needs to complete the following workstreams before 25th May 2018:

Workstreams

No	SIRO	Description	Progress	Status RAG
1	Diane Jones, Director of Quality & Safety, BHH CCGs Ben Westmancott, Director of Compliance, CWHHE CCGs	Establish a pan NWL CCGs Information Governance committee to oversee GDPR assurance and compliance	A pan-NWL CCG IG committee has been established with GDPR compliance a standing item (extending the prior BHH IG committee). A RSM audit of NWL CCGs GDPR readiness has been commissioned.	Green
2	Diane Jones, Director of Quality & Safety, BHH CCGs Ben Westmancott, Director of Compliance, CWHHE CCGs	Appoint a 'Data Protection Officer' for NWL CCGs (note that a DPO can be shared between organisation and hence a NWL DPO could provide support to GPs, federations etc. subject only to workload	A DPO job description has been graded (8A) and recruitment processes will begin subject to necessary approvals as this is a new role. In the interim the BHH IG Manager is supporting DPO activities to achieve compliance	Amber
3	Bill Sturman, Director of Informatics, NWL CCGs	Ensure that NWL CCGs 'Information Sharing Agreements' (ISAs) are compliant with GDPR. The NWL digital ISA underpins information sharing in systems such as 'Whole Systems Integrated Care'	A professional review of the NWL digital ISA is underway with the expectation of a GDPR compliant version being available at the end of March 2018. This will allow sufficient time for GPs	Green

		(WSIC) and the 'Care Information Exchange' (CIE).	and other parties to re-sign the agreement using the Data Controller Console. A 'Privacy Impact Assessment' on the new ISA has also been commissioned	
4	Bill Sturman, Director of Informatics, NWL CCGs Laurie Slater, Clinical IG Lead, CWHHE CCGs	Ensure that GPs are conversant with GDPR (training and support) and compliant with its implications for patient data (e.g. 'Fair Processing Notices')	A series of evening sessions for GPs about GDPR/ ISAs was run in February. Further communication and advice to GPs will follow during March, April and May building upon discussions with the LLMC.	Green
5	Bill Sturman, Director of Informatics, NWL CCGs	Information security review in relation to the security of personal data and the security of information processing	Following a RSM audit of NWL CCGs cyber-security maturity, activities are underway to ensure full compliance with the recommendations. In addition, security training has been added to mandatory online staff training. This training will be available to GPs once a new pan-NWL website/communications platform has been implemented (procured in February 2018).	Green
6	Huw Wilson-Jones, Director Acute Contracts, NWL CCGs	Contracts review (ensure clauses around data controllers/processors/sub-processors are transparent and compliant)	Once a DPO is appointed, the post-holder will inform and support a comprehensive review of NWL contracts. In the interim the BHH IG Manager is supporting this activity.	Amber
7	To include: Maggie Gibbs, Director of HR, NWL CCGs Mary Mullix, Director for Quality, Nursing and	Ensure internal CCG departments which hold personal data are GDPR compliant. This includes documenting the purposes of holding data, records of processing activities and breach reporting	Once a DPO is appointed, the post-holder will draft the guidelines and assurance activities necessary for relevant CCG departments to complete. In the interim the BHH IG Manager is supporting this activity.	Amber

Paper: 15

	Patient Safety, CWHHE			