

A large, thick teal-colored arc that starts from the left edge of the page and curves upwards and to the right, ending at the right edge. It frames the central text.

Q4 DPO Report 2019-20

First Community Health and Care C.I.C

Jamie Sheldrake

April 2020

Document revision history

Date	Version	Revision	Comment	Author
Apr 2019	0.1	Draft template shared		Jamie Sheldrake
22/11/19	1.0	Half-year report	Updated for half-year report	Jamie Sheldrake
16/01/20	2.0	Q3 Report	Updated for quarter 3 report	Jamie Sheldrake / Colette Allen
20/04/20	3.0	Q4 Annual Report	Updated for annual report	Jamie Sheldrake / Colette Allen

Table of Contents

.....	1
Introduction.....	4
Data Protection Impact Assessments.....	4
Assessments reviewed.....	4
DPIA Audits	5
Data Protection Incidents and Breaches	6
Reported incidents	7
Subject Access Requests.....	8
Q3 overview.....	8
Breaches and lessons learnt	8
2019-20 DSPT Progress Report.....	8
Contracts and Agreements.....	9

Communications & Culture	10
DPO Attendance	11
Training.....	12
Advice Summary.....	12
Other DPO Activity	12
Overall Half-Year DPO Opinion.....	14

Introduction

At the beginning of the 2019-20 financial year First Community changed its information governance and data protection arrangements to commission NHS NEL information governance (NEL IG) and data protection officer (DPO) service. This annual DPO report summarises the key activities and outcomes with which First Community and NEL IG have worked together during the 2019-20 financial year and provides an oversight of organisational data protection compliance and assurance.

This report should be read alongside First Community Corporate Risk Register which contains key IG risks for the organisation and First Community Information Asset Register (IAR) and Data Flow Map (DFM) to understand the key information assets processed by First Community, the lawful basis for processing, how access is controlled and who First Community share those assets with.

This is a Board summary report of key data protection and information governance activity and issues to date and serves as First Community data protection and information governance annual assurance report. First Community operate an Information Governance Group (IGG) which meets regularly throughout the year which is attended by the First Community Senior Information Risk Owner (SIRO), the Caldicott Guardian, DPO and IG Compliance Manager. Progress against the First Community Annual DPO Compliance Plan and key IG issues are discussed in detailed in those meetings and as needed on a priority basis throughout the year.

Data Protection Impact Assessments

Assessments reviewed

Data Protection Impact Assessments (DPIA) are the means by which an organisation evidences that Privacy by Design is being implemented into new processes, services and technologies.

Review Date	DPIA Title
01/04/2019	Gypsy, Roma & Traveller Community
12/07/2019	E-Expenses

17/07/2019	E-Consent
04/09/2019	Home First
04/09/2019	Sollis
14/11/2019	EMIS Mobile
14/11/2019	GRT Immunisations
18/11/2019	Children's Weaning Workshop
21/11/2019	Vulnerable Families
21/11/2019	Clinical supervision Guidelines Review
18/12/2019	Diligent
03/01/2020	Eventbright
16/01/2020	Consultant Connect
25/03/2020	COVID-19

DPIA Audits

Article 35 (GDPR) requires a DPIA to be completed where the

“nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons [living people].”

The GDPR requires that

“The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.”

The use of a DPIA to review legitimacy, risks and controls for processing of personal and special category data is central to an organisations understanding and management of that processing and reflects a core organisational management tool that is of high interest to Senior Information Risk Owners (SIROs), Caldicott Guardians, Boards and Governing Bodies.

Not all processing or intended processing is likely to result in high risks. However, in line with national and industry recommendations and reflecting the pre-GDPR NHS mandate to complete DPIAs for all processing, it is highly recommended that a DPIA is utilised as the default tool for identifying risks and designing controls for processing of personal data.

Article 36 (GDPR) requires that the organisation consult with the supervisory authority (ICO) where a DPIA indicates that

“the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.”

Review Date	DPIA Title	Audit Date	Recommendations implemented?
03/12/2019	Gypsy, Roma & Traveller Community	December 2019	Yes
18/12/2019	E-Expenses	December 2019	Yes
01/11/2019	E-Consent	December 2019	Yes

Data Protection Incidents and Breaches

An overall summary of incidents logged throughout the year. Further details provided on serious incidents which have required logging on DSPT and notified to ICO.

In May 2019 the DPO reviewed the organisational Serious Incident Policy to bring it into line with post GDPR / DPA 2018 requirements and to meet the latest NHSD national data breach guidance.

Category		DSPT Recorded/ Non-ICO Reportable	ICO Reportable
1.	Personal Confidential Data	0	0
2.	Staff Responsibilities	0	0
3.	Training	0	0
4.	Managing Data Access	0	0
5.	Process Reviews	0	0
6.	Responding to Incidents	0	0
7.	Continuity Planning	0	0
8.	Unsupported Systems	0	0
9.	IT Protection	0	0
10.	Accountable Suppliers	0	0

Reported incidents

First Community have a high awareness when it comes to incident reporting and are keen to capture all incidents, implementing lessons learnt. In the financial year 19-20, First Community

have recorded 71 IG related incidents, none of which have required reporting on the DSPT or to the ICO.

Subject Access Requests

Q4 overview

There have been 170 subject access requests received in the financial year 2019-20. There has been a significant increase in the number of subject access requests received for the financial year 2019-20 for which there are two identified causes; the increase in SARs since the implementation of GDPR as is demonstrable across the sector and the centralisation of the subject access request procedure ensuring all subject access requests are now being identified and appropriately recorded.

The IG Compliance Manager and the DPO have delivered extensive training to individual's, service leads, directors and individual teams to ensure a significant improvement in the internal knowledge base in order to enable First Community to manage a compliant subject access request service, with support from NEL IG.

Breaches and lessons learnt

There has been a total of 3 breaches in timeframes with regards to subject access requests; all of which occurred in Q1 at a period of staff change. At this point in time gaps in the service were identified and the IG Compliance Manager along with senior members of internal staff worked to review the subject access request process as a whole. The IG Compliance Manager created a revised process to accommodate the needs of the business and combined with the realignment of the service and ongoing and significant training within the organisation, no further breaches have occurred. There have been no complaints to the ICO this year to date.

2019-20 DSPT Progress Report

Under current NHSD guidance, there is no requirement for First Community as a community interest company to carry out an independent audit in relation to the Data Security and Protection Toolkit. However, following discussion between the IG Compliance Manager and the SIRO, it was agreed that RSM would be commissioned to conduct an audit w/c 21 October 2019 in order to ensure First Community were on track to obtain a high level of assurance at the point of toolkit submission at year end.

RSM audited a total of 10 assertions, made up of 27 requirements. Of these requirements 3 recommendations were received all of which were categorised as low priority.

- Information Asset Registers are due for final sign-off in January 2020 ahead of submission in February/March.
- One due date was missing from the workplan although this was agreed with the auditors for completion by end December 2019
- While there is no requirement and it is not possible, to upload information directly to the toolkit for some requirements, it was suggested it may be useful to provide a link in some of the comment boxes going forward.

Overall, there were no medium or high priority areas of concern for completion in the toolkit and First Community has been assessed as being in a reasonable position for progression towards year end.

First Community's DSPT was published on time meeting all the mandatory requirements for 2019-20.

Contracts and Agreements

Summary of contracts reviewed and any learnings.

Date	Activity
24/06/2019	SECAMB IBIS Information Sharing Agreement reviewed with recommendations for changes / improvements.
01/11/2019	Children and Family Health Surrey
14/11/2019	Heart Failure Service
26/11/2019	Vulnerable People Reporting System (SCC Emergency Resilience) DSA reviewed following GDPR refresh at request of Chief Nurse.
March 2020	DPO review of and recommendation to sign new Surrey Care Record Information Sharing Agreement.

Communications & Culture

Date	Activity
02/04/2019	Staff comms announcing availability of NEL IG Help Desk & the help available.
17/04/2019	Staff comms advising IG policies are now available
02/05/2019	Office move guidance sheet for all staff
30/05/2019	Sending emails securely – How to Guide/Dos and Don'ts
30/05/2019	Sending Post Securely (internal and external) - Internal mail process/How to Guide
13/06/2019	IG Incidents – How to spot an IG Incident/What to do
04/07/2019	Subject Access Requests – Procedure/Process Flow, SAR Guidance, Data Subject Rights
04/07/2019	Data Protection Officer (DPO) – DPO Guidance/Role and Responsibilities/Contact Details
25/07/2019	Privacy Notices – Data Subject Rights
10/10/2019	DPIA Procedure/Protocol/Policy
10/10/2019	Information Assets and Data Flows
10/10/2019	Reminder to Lock Screens

10/10/2019	Safe Email Guidance
10/10/2019	Phishing Emails
10/10/2019	DSPT Updates/audits/big picture guides
11/11/2019	Minor Injuries Unit – Safeguarding Guidance
05/12/2019	CFHS Newsletter – When to Share Information/SAR Guidance
February 2020	Staff reminder for Training Completion
March 2020	COVID-19 updates and guidance to support all functions of the organisation.

Other DPO Engagement

Date	Activity
29/05/2019	Attendance at First Community Information Governance Group
20/06/2019	Attendance at First Community Audit Committee
22/11/2019	Half-year SIRO / DPO discussion on DPO perspective of progress made within year with recommendations for action.
17/01/2020	Q3 SIRO / DPO discussion on DPO perspective of progress made within year.
20/04/2020	Annual DPO data protection compliance and assurance report.

Training

Date	Training Activity
09 May 2019	Finance team development day
05 June 2019	Annual Board IG training
08 July 2019	Annual Caldicott Guardian training
12 Aug 2019	Annual SIRO training
03 Oct 2019	SAR training for First Community Heads of Service
4 Nov 2019	Additional annual Board IG training session
4 Nov 2019	SAR Workshop - Safeguarding
12 Dec 2019	SAR Training – Review
19 Dec 2019	Record Keeping Training

All-staff IG training was achieved at 96.4% for the financial year 2019-20.

Advice Summary

A summary of advice provided throughout the year is recorded on NEL IG Help Desk logs.

Other DPO Activity

Date	Activity
01/04/2019	Register NEL CSU as DPO for First Community with the ICO

02/04/2019	IGG Terms of Reference Review
24/04/2019	Annual DPO Work-plan discussed & agreed with SIRO
25/04/2019	Organisational Assessment for DPO requirement completed for First Community
09/05/2019	2018/19 annual DPO report reviewed with recommendations
17/05/2019	DPO review of First Community Serious Incident Policy to bring into line with latest and post GDPR / DPA 2018 NHSD Notification of Data Security and Protection Incidents national guidance.
20/09/2019	Attendance at Kent/Surrey/Sussex CIO Forum at request of AB.
23/05/2019	Annual IG / Data Protection Audit Plan created – subsequently discussed at the IG Group on 29 May 2019.
24/09/2019	Correspondence with John Hodson – national lead for DSPT – for clarification regarding correct DSPT category for First Community to complete as advice issued recommended category 3 but national documentation recommended category 1. Confirmation received from John Hodson that category 1 is for Trusts only and confirmation that national documentation which advised Community Interest Companies should complete category 1 would be amended and re-issued.
25/09/2019	DPO review of revised Sussex Wide ISP to which First Community are a signatory.
Dec 2019	Final DPO review of IG Compliance Manager refreshed First Community IG Policies (IG Framework, Information Governance, Information Management, IT Security, Data Quality, Acceptable Use)

Jan 2020	DPO review of Information Asset Owner Handbook updated for DPA2018, GDPR and Data Security and Protection Toolkit requirements.
----------	---

Overall Annual Summary and Opinion

Throughout the 2019-20 year First Community have been enthusiastic and proactive in embedding and improving their organisational practices and culture with regards to data protection operational working and culture. This has been reflected primarily through First Community close-working and engagement with their NEL IG Compliance Manager who has worked as a key member of the organisational governance structure and who's operational input has driven this forward and for which they received runner up partner of the year award.

Particular note should be given to the engagement by the organisation with Data Protection Impact Assessments, their commitment to and achievement of organisational information governance training and their determination in upholding data subject rights and freedoms as described within GDPR / Data Protection Act (2018), and in particular subject access requests which often poses significant challenges for most organisations.

Through their continued and practical close engagement with the IG Compliance Manager and Data Protection Officer and their achievement of all mandatory requirements of the Data Security and Protection Toolkit, First Community can reflect a sincere organisational commitment to embedding data protection within their organisation.