2022-23 First Community

Annual Information Governance & DPO Report

Revision history Document

Date	Version	Revision	Comment	Author
July 2023	0.1	Issued	Issued	Milton Shoriwa

Contents

1. Introduction

This is the First Community Information Governance (IG) Annual Report for the 2022-23 DSPT reporting year. This report provides an overview of the organisation's data protection and information risk management activities.

First Community operates an Information Governance Group (IGG) chaired by the Senior Information Risk Owner (SIRO) and includes key representatives, the service leads or representatives, the Data Protection Officer, and the IG Consultant/Compliance Manager. The IGG ensures the effective implementation of the organisation's IG framework and addresses relevant issues throughout the year.

Key Messages

- First Community achieved "Standards Exceeded" compliance with the IG standards set by the NHS Data Security and Protection Toolkit (DSPT) for 2022-23.
- DSP Toolkit Internal Audit outcome was "Substantial Assurance with no improvement recommendations".
- No significant personal data-related incidents were reported or notified to the Information Commissioner's Office (ICO), resulting in no regulatory action against First Community.

2. Data Security and Protection Toolkit (DSPT)

The DSPT, provided by NHS England, supports IG compliance and monitoring in NHS organisations. It helps us demonstrate compliance with mandatory data security and protection standards. The DSPT covers 10 sections aligned with the National Data Guardian (NDG) Standards.

Self-Assessment Results for 2022/23

First Community successfully met all mandatory assertions in the DSPT, resulting in a "Standards Exceeded" outcome. The organisation's approved 2022-23 DSPT implementation plan was fully implemented, and all planned activities were completed prior to the DSPT self-assessment submission. Throughout the year, First Community made progress in further developing processes and embedding information governance principles within the organisation.

Information Governance Group (IGG) meetings were held regularly to monitor progress against the annual DSPT workplan.

The IG team will continue leading and demonstrating progress in the coming year to ensure compliance with the 2023-24 standards.

DSPT Internal Audit

An internal audit of the 2022-23 DSPT self-assessment was conducted to assess First Community's compliance with the DSPT. The audit aimed to identify any risks or areas

for improvement in the organisation's data security and protection practices and to assess the quality of the DSPT evidence prior to submission.

The IGG is pleased to report that the internal audit found no risks associated with the DSPT assessment. The outcome of the audit provided substantial assurance, indicating that First Community's data security and protection measures are robust and effective.

The internal audit report did not include any recommendations for improvement, further affirming First Community's commitment to maintaining a high standard of information governance. This positive outcome reflects the dedication and efforts of First Community staff in implementing and adhering to best practices in data security and protection.

The organisation will continue to prioritise regular internal audits to ensure ongoing compliance and identify opportunities for improvement in the organisation's information governance practices. The successful internal audit outcome reinforces the organisation's commitment to safeguarding the confidentiality and integrity of the data entrusted to the organisation by our patients and stakeholders.

3. Policies and Procedures

First Community has established comprehensive policies data protection and security policies and procedures, including data breach management, data subject rights, and privacy impact assessments, to ensure adherence to relevant data protection principles.

The organisation continues to effectively implement all its information governance policies and procedures. All policies and procedures have been reviewed and are up to date. The information Governance Group continues to monitor and review all the organisation's IG policies.

4. Information Risk Management

The Information Governance Group, chaired by the SIRO, maintains regular scrutiny of data protection and other information governance risks. The Risk Register is maintained and routinely discussed at each IGG meeting, and processes are in place for risk escalation.

Throughout 2022-23 First community did not have any high risks requiring significant mitigation resources.

Staff Training & Awareness

First Community provided online mandatory data protection training to all staff, ensuring staff understand their responsibilities in handling personal data and are aware of key data protection principles, rights of data subjects, and best practices for data security.

The NHS mandatory requirement for information governance training is for a total of at least 95% of staff to complete the mandatory training annually. First Community continues to comply with this training requirement.

Awareness Campaigns: First Community conducted awareness campaigns to promote a strong data protection culture within the organisation. These campaigns included communication materials, workshops, and interactive sessions to reinforce the importance of data protection among staff members. As part of this campaign, the organisation continues to implement a programme of site confidentiality audits to identify and assess any possible information governance risks across First Community sites. Staff who work remotely are also required to complete confidentiality self-assessments with reports of any risks submitted to the information governance group meetings.

5. Data Protection Assurance

Processes for Handling Data Subject Requests

First Community has implemented efficient procedures to handle data subject requests, including access, rectification, erasure, restriction, and objection. These processes ensured that data subjects' rights were respected, and responses were provided within the required timeframes.

First Community remains committed to complying with SARs. During the reporting year, we received a total of 159 SARs, with a compliance rate of 99.37%. Only one request was responded to a day after the statutory deadline due to staffing shortage caused by COVID.

Privacy Notices

The First Community Privacy notice is regularly reviewed and updated. It is regularly reviewed to ensure transparent communication with patients or data subjects regarding the processing of their personal data. The privacy notice clearly outlines the purposes, legal basis, data retention periods, and data subject rights.

Data Protection Impact Assessments

First Community has fully implemented Data Protection by design processes to ensure compliance with the Data Protection Act 2018/UK GDPR. Data Protection Impact Assessments (DPIAs) are conducted to assess information and data protection risks associated with implementing new systems or technologies. Staff are reminded to complete DPIA forms for new projects or significant changes impacting personal confidential information.

The organisation conducted DPIAs for high-risk processing activities to identify and mitigate potential privacy risks. This included assessing the necessity and proportionality of data processing, implementing appropriate safeguards, and involving relevant stakeholders in the decision-making process.

During 2022/23, no DPIAs involving high-risk processing of personal confidential data required notification to the ICO.

Title	Department	Project Description
Discharge Medicine Service	Medicines Management	Discharge Medicines Service is part of several measures being introduced as part of the second year of the NHS 5-year plan to ease pressures on A&Es
Electronic Prescription Service	Project Management Team	E-prescribing allows prescribers to send prescriptions electronically to a pharmacy of the patient's choice.
East Surrey Place based public involvement group	Project Management Team	Exploring the possibility of extending the Patient Network to East Surrey Place,
Vulnerable Persons Reporting System – System replacement	Surrey County Council	Live data testing DPIA for the VPRS replacement system. Not possible to use dummy data so DPIA was carried out data controllers asked to review and approve DPIA for live data testing.
Kabi	IT/Clinical	Patient information will be shared with Fresenius Kabi via an online portal. This information is currently shared using a paper/ e-mail-based system.
Manual OH Referral Process	Occupational Health	Transfer from Cohort system to Orchid Live

6. Caldicott Report

- In 1997 Dame Fiona Caldicott led a review to respond to concerns over the use of patient data.
- The 1997 report is '[The Caldicott Committee's Report on the Review of Patient-Identifiable Information]' and established the six original Caldicott Principles with a seventh added in 2013 and eighth in December 2020.
- A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.
- Since 1999, all NHS organisations must have a Caldicott Guardian whose details are on the Caldicott Guardian Register First Community have two guardians on the register, this ensures no single point of failure and support and challenge for complex cases:
    - Jon Ota, Caldicott Guardian
    - Emma Marcroft, Deputy Caldicott Guardian
- This section of the Information Governance Annual report provides a summary of activity for the Caldicott Guardians.

2022 / 23 Caldicott Issues

The table below shows the Caldicott requests for the past five years:

	2017 / 18	2018 / 19	2019 /20	2020 / 21	2021 / 22	2022/23
Number of Caldicott Approvals	4	5	13	14	7	4

The table below shows the nature of these requests:

	2017 / 18	2018 / 19	2019 /20	2020 / 21	2021 / 22	2022 / 23
National Audit	2	4	3	0	1	0
Subject Access Request	0	0	2	1	2	2
Emergency Planning	0	0	2	0	0	0
NMC	0	0	2	0	0	0
Data / EMIS	0	0	4	9	3	0
LeDer	0	0	0	1	0	0
Access to Health	0	0	0	3	0	
Information Sharing	2	1	0	0	1	1
Safeguarding	0	0	0	0	0	1

- The number of Caldicott requests decreased in the past year after increases over the previous two years. The Caldicott Guardian continue to support complex subject access requests.
- The national audit requests in previous years were for ongoing data entry, there has been no new national audit requests for this year.

7. Data Protection Incidents and Breaches

First Community maintained a robust data breach management process, including incident reporting, investigation, and notification procedures. Any identified data breaches were promptly reported and investigated in line with the NHS procedures and ICO reporting requirements.

In 2022/23, 48 information governance incidents or near misses were recorded. No significant personal data breaches were reported or notified to the ICO. No complaints were made to the ICO by the public during this period.

8. Ongoing Initiatives and Future Plans

a. **Privacy by Design and Default:** First Community continues to implement privacy by design and default principles in the development and implementation of new systems, processes, and services. The organisation has effectively expanded its focus on conducting DPIAs for new projects, services, and technologies to proactively identify and address privacy risks. This approach ensures that privacy and data protection considerations are integrated from the outset. The information governance team supports staff in completing DPIAs and managing any risks that are identified.

b. **Data Protection Training and Awareness:** The organisation will continue to focus on delivering training to all its staff and to ensure that all staff that need specialised training continue to get the support they need through the information governance team. The IG team will review the training needs for staff and support the organisation in providing effective information governance training to staff.

   The organisation will continue to provide regular data protection training and awareness campaigns to maintain a strong data protection culture and keep staff informed about evolving data protection requirements.

c. **Third Party Contracts:** First community will continue to strengthen its contract review processes, ensuring that all third-party relationships align with the organisation's data protection requirements and that appropriate safeguards are in place to protect personal confidential data. As part of the 2023-24 DSP Toolkit self-assessment, the organisation is going to review all contracts with third parties that involve the processing of personal data. This will be one of the key elements of the 2023-24 DSP Toolkit work plan.

d. **Regulatory Compliance:** The information governance team will closely monitor regulatory developments and updates in data protection laws to ensure ongoing compliance. This includes staying informed about any changes in applicable regulations, guidelines, or interpretations that may impact our data protection practices.

e. **Data Protection Awareness for Patients:** Where necessary First Community will develop targeted communication initiatives to educate patients about their rights, the importance of data protection, and how their personal data is handled within the organisation. This will largely be done through the privacy notices, but any new services or pathways may require targeted communication initiatives. The information governance team will continue to work with the comms team to ensure appropriate IG communication materials are shared with patients and staff.

9. Conclusion

First Community has made significant progress in its data protection efforts over the past year. The organisation has demonstrated a commitment to safeguarding personal data, complying with applicable regulations, and promoting a strong data protection culture within the organisation as indicated by the excellent results of the DSP toolkit internal audit.

The organisation has achieved compliance with the mandatory IG standards set by the DSPT for the 2022-23 reporting year. No significant personal data-related incidents or breaches were reported, demonstrating the organisation’s commitment to information security and data protection.

First Community has maintained a high level of compliance with SARs, ensuring individuals' rights to access their personal data and will continue to prioritise information governance and risk management to uphold the confidentiality of patients' information.

As Data Protection Officer, I would like to thank all staff members for their dedication to information governance and their commitment to protecting personal data. By embedding IG principles into daily practices, staff ensure the ongoing security and privacy of the data entrusted to the organisation.

However, data protection is an ongoing process, and First Community must continue to prioritise and invest in information governance initiatives to maintain the trust of its patients, protect their privacy rights, and ensure the secure handling of their personal information.