Information Governance Report 2021-22

First Community Health and Care C.I.C

July 2022

Document revision history

Date	Version	Revision	Comment	Author
July 2022	0.1	Draft	Initial Draft	Milton Shoriwa
July 2022	0.2	Draft	Minor changes. SIRO review	Milton Shoriwa/ Adrian Baillieu (SIRO)

Contents

Introduction

This is the Information Governance (IG) Annual report providing key information governance activity and issues for the 2021-22 reporting year. The report covers the First Community Health & Care CiC's (First Community) data protection and information risk management assurance activity.

First Community operate an Information Governance Group (IGG) which meets regularly throughout the year. The IGG is an assurance group responsible for ensuring that the First Community IG framework is effectively implemented. The IGG is chaired by the by the First Community Senior Information Risk Owner (SIRO) and its membership includes the Caldicott Guardian, representatives from key areas within the organisation, the Data Protection Officer and the IG Compliance Manager.

Progress against the First Community's implementation of its approved IG framework associated annual workplans and IG issues and risks make up the key agenda items of the IGG and are discussed in detailed in the IGG meetings as necessary on a priority basis throughout the year.

Key Messages

- First Community met the mandatory IG compliance standards set out in the NHS Data Security and Protection Toolkit (DSPT) for the 2021-22 reporting year.
- No significant personal data related incident was reported and notified to the Information Commissioner's Office; therefore, no regulatory action was taken against First Community.
- Moving many staff to homeworking created additional information security risk, however, no significant increase in incidents was evident.
- 99.37% of Subject Access Request were responded to within the statutory deadline of 30 calendar days.

Data Protection and Security Toolkit (DSPT)

The Data Security & Protection Toolkit (DSPT), which was introduced in 2018 and has been provided by NHS Digital to support NHS organisations' IG compliance and monitoring helps to provide evidence that First Community is compliant with the mandatory data security and protection standards that have been set for the organisation.

The DSPT is made up of 10 sections that cover the compliance with the 10 National Data Guardian (NDG) Standards.

Self-Assessment Results for 2021/22

This report covers First Community performance against its Information Governance responsibilities during the financial year 2021/22. For the past couple of years, the DSPT submissions deadline has been moved from end the 31st of March 2021 to the 30th of June each year.

First Community met all the mandatory assertions and achieved a 'Standards Met' outcome.

The organisation managed to implement its approved 2021-22 DSPT implementation plan and all the activities in the action plan were completed prior to the organisation's submission of the DSPT self-assessment.

Throughout 2021/22 progress was made in the DSPT to further develop processes and ensure that information governance principles and understanding continue to be embedded throughout First Community.

Below are the components of the DSPT assertions which covers the First Community mandatory compliance requirements:

- NDG 1 - Personal confidential data
- NDG 2 - Staff responsibilities
- NDG 3 - Training
- NDG 4 - Managing Data Access
- NDG 5 - Process Reviews
- NDG 6 - Responding to Incidents
- NDG 7 - Continuity Planning
- NDG 8 - Unsupported Systems
- NDG 9 - IT Protection
- NDG 10 - Accountable Suppliers

The Information Governance Group (IGG) continues to hold regular meetings to monitor progress against the agreed annual DSPT workplan. The IG team will continue to lead and demonstrate progress with the First Community IG workplans to ensure the 2022-23 standards are met as well.

Information Risk Management

The Information Governance Group, which is chaired by the First Community's Senior Information Risk Owner (SIRO), maintains regular scrutiny of the risks associated with Information Governance. The Risk Register report is routinely discussed at each Information Governance Group meeting and processes are in place for escalation of events and risks. There are currently no high risks requiring employment of significant mitigation resources on the risk register.

Data Protection Impact Assessments

First Community has fully implemented the Data Protection by design processes within the organisation to ensure the organisation's compliance with Data Protection Act 2018/UK GDPR compliance. Data Protection Impact Assessments (DPIA) are how organisations evidence that Privacy by Design is being implemented into new processes, services, and technologies. DPIAs help the organisation to assess the information and data protection risks that may be associated with implementing new systems or technologies within First Community.

All staff have been made aware of the DPIA process and are regularly reminded to complete the DPIA form for any new projects and any significant changes to projects or activity that may have an impact on personal confidential information

During 2021/22 First Community did not have any DPIA that involved high risk processing of personal confidential data requiring notification to the Information Commissioner's Office.

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.

2021 / 22 Caldicott Issues

- The table below shows the Caldicott requests for the past four years:

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

- The table below shows the nature of these requests:

	2017 / 18	2018 / 19	2019 /20	2020 / 21	2021 / 22
National Audit	2	4	3	0	1
Subject Access Request	0	0	2	1	2
Emergency Planning	0	0	2	0	0
NMC	0	0	2	0	0
Data / EMIS	0	0	4	9	3
LeDer	0	0	0	1	0
Access to Health	0	0	0	3	0
Information Sharing	2	1	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.
- The national audit requests in previous years were for ongoing data entry, there has been one new national audit request for this year.
- During 2020 / 21 the Caldicott Guardian noticed an increase in requests for EMIS / Data approvals so supported the Performance and Business Intelligence Manager to undertake

a review of the implementation of the policy. This has led to increased governance through CSAG and the appointment of a Privacy Officer, there is a notable decrease in requests this year.

Data Protection Incidents and Breaches

Robust processes are in place to ensure that information security breaches are appropriately recorded and effectively managed in line with Data Protection Legislation and organisational procedures.

A total of 45 information governance incidents or near misses were recorded during 2021/22. The First Community IGG routinely receives and scrutinises information security/IG incidents reports.

Throughout the year no significant personal data breach was reported and notified to the Information Commissioner's Office, therefore, no regulatory action was taken against First Community.

First Community did not also receive any complaints made to the ICO by a member of the public in the same period.

The organisation continues to maintain the commitment for staff training and adhering to processes and good practice to minimise the recurrence of staff errors that can lead to significant data breaches which may have an adverse impact on patients and the organisation.

Subject Access Requests

The right of access or Subject Access Requests (SARs) are the principal data subject right enshrined within UK GDPR. It gives individuals the right to obtain a copy of their personal data, as well as other supplementary information and helps individuals to understand how and why the organisation is using their data, and check if the organisation is doing it lawfully.

SARs have a legal response timeframe of a calendar month within which individuals expect to receive a copy of the data held about them by an organisation.

First Community continues to comply with the statutory SARs. The organisation received a total of 157 SARs during 2021-22. Only a single request was responded to a day after the statutory deadline because of staff shortage due to COVID.

First Community's compliance rate of 99.37% is a good indicator of how well personal data is managed or handled within the organisation.

Information Risk Management Strategy

First Community continues to effectively manage information risks across the organisation. Risks are monitored by the First Community's IG Group.

As part of the information risk strategy the organisation has implemented several operational procedures and operational activities which include the implementation of the Data Protection Impact Assessments for new projects and changes to projects or activity that impacts the processing of personal data.

During the 2021/22 DSP Toolkit reporting year several IG spot-checks were carried out to support the organisation IG assurance, compliance and identify any risks. First Community staff continue to assist the IG Team in undertaking confidentiality spot-checks across First Community estate to support the identification of IG risks and their management or mitigation.

The spot-checks/confidentiality audits covered the following sites:

- Caterham Dene Hospital
- The Health Centre - Birchwood Medical Practice
- Wayside
- Oxted Therapies Unit
- Forum House
- Phoenix House
- Audiology, Crawley
- South Tandridge District Nursing Team/ Tandridge District Council Offices

The confidentiality spot-checks/audits did not show any significant risks for personal data identified which continues to reflect a strong IG culture that encourages the protection and maintenance of the confidentiality of service user information.

However, there continues to be some confidentiality risks around shared spaces with other public services or local authorities where premises are shared across services. But First Community staff within such spaces are aware of the IG policies and procedures to follow which are made available through the First Community intranet. The organisation also continues to meet the 95% target for IG training for all staff which provides assurances that staff are aware of the need to maintain confidentiality and protect service user information.

Training

First Community continues to implement an effective training plan to ensure that all staff receive appropriate IG training relevant to their role within the organisation. The organisation has managed to achieve the required 95% mandatory training requirement for all organisations that deliver NHS services.

In addition to the mandatory training relevant IG training was delivered for key roles within the organisation during 2021/22.

The following training was provided to support the organisation's information governance framework.

- Annual Board IG training
- Annual Caldicott Guardian training
- Deputy Caldicott Guardian training
- SIRO training

Overall Annual Summary

First Community has remained committed to building a good information governance culture within the organisation. This is also supported by the organisation's continued success in meeting mandatory 95% IG training requirement and the implementation of the IG training plan ensuring that key staff within the organisation receive information governance training relevant to their role.

The commitment of First Community to maintain good standards of practice and engagement with data protection principles is commendable. The risk-based IG approach which is implemented though the DPIA and the IG Group processes ensures that the organisation can monitor and manage IG risks as well as comply with statutory and regulatory requirements.