Privacy Impact Assessment Policy and Procedure

Statement & Purpose of Policy

This document sets out Serenta Homecare Homecare policy in respect of Privacy Impact Assessments.
The policy details the mandated process to be followed to ensure a formal assessment is completed to determine whether any proposed changes to Serenta Homecare processes and/or information assets impact on the integrity and accessibility of personal information.
Some of the considerations that should be taken into account are whether a new process or information asset will:

- Affect the quality of personal information already collected;
- Allow personal information to be checked for relevancy, accuracy and validity;
- Incorporate a procedure to ensure that personal information is disposed of through archiving or destruction when it is no longer required or in accordance with the Records Management NHS and social Care Code of Practice;
- Have an adequate level of security to ensure that personal information is protected from unlawful or unauthorised access and from accidental loss, destruction or damage;
- Enable data retrieval to support business continuity in the event of an emergency;
- Enable the timely location and retrieval of personal information to meet a subject
- access request;
- Affect the way in which the commissioner captures information within / monitors information from a key system.

It should be recognised that changes to processes and information assets may also be driven by service changes, such as a new service being commenced.

Scope

This policy reinforces the principles of Information Governance and Data Protection applied to Serenta Homecare and its services. The document outlines Serenta Homecare's approach and methodology for Privacy Impact Assessments for new and existing systems and processes.
The policy applies to information held in both manual and electronic form.
This policy applies to all staff who work for Serenta Homecare, including contractors and those who are responsible for project managing a new project, implementation of a new process or plan to modify a current system (information asset).

Background

It is best practice to ensure that all new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured

manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements.

Privacy Impact Assessment (PIA) and Process

A PIA must be carried out in addition to compliance checking or a data protection audit, and conducted at a stage when the outcome can genuinely affect the development of a project or process. An effective PIA will help identify and avoid problems which may not be obvious at the conception stage and should form an intrinsic part of the overall risk assessment. To summarise, the rationale for conducting a PIA is to:

- Identify and manage risk;
- Avoid unnecessary costs and inadequate solutions;
- Avoid loss of trust and reputation;
- Meet legal requirements in terms of information security, data protection and confidentiality.

There are two levels of PIA:

Initial Screening / Small Scale PIA

A small-scale PIA process involves the analysis of privacy issues, but is less formalised; requires less information gathering; involves less investment; and is more likely to focus on specific aspects of a large-scale project rather than a project as a whole. The Initial Screening Questionnaire is based on the Small Scale PIA.

Full Scale PIA

A full-scale PIA conducts a more in-depth internal assessment of privacy risks and liabilities, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them.

When should a PIA be undertaken?

Not every new project, system or change in process will require a PIA. The Information Commissioner's Office recommends that PIAs are completed to comply with a change in law, introduction of new or intrusive technology or where private or sensitive information which was originally collected for a limited purpose is going to be reused in a new and unexpected way. Completion of the Initial Screening Questionnaire will ensure that a PIA is completed only when necessary and provide evidence to support Serenta Homecare quality assurance processes.
Best practice dictates that the initial screening questionnaire should be started when:

- The project / process is being designed and the scope has been agreed;
- Before a system has been procured;
- Before contracts/MOUs/agreements have been signed.

Who is required to complete a PIA?

The initial screening questionnaire should be completed by the Information Asset Owner (IAO) or delegated to the individual responsible for overseeing the implementation of the project / process / amendment to an existing system.

Applying the Outcome of the Initial Screening Questionnaire / Small-Scale PIA
Where answers to questions are 'Yes', consideration should be given to the extent of the privacy impact and the resulting project risk. The greater the significance, the more likely that a full PIA will be required.

Roles and Responsibilities

The Board - owns the Information Risk Policy and the implementation of measures to minimise information risk and must safeguard the interests of staff, patients and information assets of Serenta Homecare.

Senior Information Risk Owner (SIRO) - is responsible for ensuring an Information Risk Policy is developed, implemented, reviewed and its effect monitored. Privacy Impact Assessment is one element of the management of information risk, which should be managed in accordance with the Assurance Framework.

The Information Governance Lead will:

- Take delegated responsibility for Serenta Homecare's information risks;
- Act as the advocate for information risk;
- Provide written advice to the Managing Director, as required
- Occupy a key role in ensuring effective management and identification of information risks.

Information Asset Owners are senior individuals involved in managing particular aspects of Serenta Homecare's business. Their roles include:

- Understanding what information is held;
- Knowing what is to be added and removed;
- Knowing how information is moved / transferred;
- Knowing who has access and why;
- Ensuring compliance with the relevant legal frameworks, i.e. consent and confidentiality

As a result they are able to understand and address potential risks to the information assets they 'own' and to provide assurance to the SIRO concerning the security, confidentiality, integrity and use of assets.

Information Asset Administrators (IAA) support IAOs by ensuring:

- Policies and procedures are followed;
- That actual or potential security incidents are recognised and reported;
- Consultation with their IAO on incident management occurring; and that
- Information Asset Registers are up to date.

The Board will formally monitor the implementation and performance of this policy by:

- reviewing highlighted risks in the Corporate Risk Log
- considering IG risk mitigation plans;
- ensuring a programme of internal/external audit reviews;
- monitoring the implementation of audit recommendations.

This policy will be reviewed two yearly by the IG lead.

Document Control

Date Approved: June 2026
Target Audience: All Serenta Homecare Homecare Staff
Review Date: June 2028
Author: Fran Beardsmore