

Battersea Healthcare CIC GDPR Statement

Battersea Healthcare CIC Summary of IG arrangements in preparation for General Data Protection (GDPR) and relevant audit to provide assurance of information governance within Battersea Healthcare CIC – the Wandsworth GP Federation.

History

Updated by Nargis Khan 17/04/2018

Finalised by Jim Fenwick 24/05/2018

To be reviewed and confirmed at IGC in May 2019

1 Purpose

- 1.1 To advise how Information Governance is managed within Battersea Health Care, the approach to GDPR compliance and any audits to provide assurance of good IG.

2 IG Management

- 2.1 The Company Battersea Healthcare CIC defines the organisations information governance (IG) model, considering legal and NHS requirements.

Tom Bailey (board member) is the Battersea Healthcare CIC's Caldicott Guardian.

SIRO is Nargis Khan (board member),

The IG Group has oversight of the IG work programme, compliance with standards and the law, risk, incidents, training, information sharing and the IG Toolkit submission. The IG Group meets quarterly (depending on the time of year), chaired by SIRO.

Battersea Healthcare CIC have a dedicated IG team who support the organisation to manage confidentiality, security and data quality using the NHS Digital IG Toolkit, our annual submission against the toolkit has been satisfactory for the last five years. Each toolkit submission is subject to internal audit, and substantial assurance has been found each year. Battersea Healthcare CIC is registered under the Data Protection Act 1998 (registration no Z2254511).

Battersea Healthcare CIC has very strong and established processes for IG serious incident reporting, investigation and lessons learnt as part of the organisations Serious Incident policy. Incident reporting occurs with each IG incident identified to the IG Team and the CIO/ SIRO to determine whether they warrant a serious incident panel to determine immediate actions to be taken and to commission an investigation for learning purposes.

3 GDPR

- 3.1 GDPR implementation is being carried out by the IG Team as part of the IG Department work program overseen by the IG Group in advance of the regulations coming into force on 25 May 2018.

Battersea Healthcare CIC implementation plan is made up of a number of key areas which have been highlighted by the Information Commissioner's Office (ICO) and these have formed the basis of our organisations implementation activities. The areas identified include: awareness, information held by the organisation, communicating privacy information, individual's rights, subject access requests, lawful basis for processing personal data, consent, children, data breaches, data protection by design and data protection impact assessments, data protection officers, and international transfers.

The Information Commissioners Office (ICO) provide a self-assessment checklist for GDPR compliance, Battersea Healthcare CIC assessment resulted an overall amber rating, we are working through the plan to take this to green.

GDPR is a standing item on the Information Governance Committee (IGC) agenda and the IGC has overseen a number of activities which have already been carried out including updates to our organisation's Notice, a review of the Subject Access Request (SAR) policy, creation of a Data Protection Impact Assessment (DPIA), appointment of a Data Protection Officer (DPO) and the communication and discussion of guidance with Trust colleagues in relevant departments such as Patient Safety/Incidents, IT & Clinical Systems, Research & Audit, Safeguarding, etc.

A number of activities will conclude to achieve compliance by May 2018, these are:

- Conclude the review of internal and external data flows and risk assessment
- Analysis of (expected) European and National level guidance in relation to Consent and findings to be reported to IGC.
- Review of contracts (especially in relation to the use of sub-processors) to ensure they are GDPR compliant

4 Audit

4.1 There are a number of areas of audit that provide Battersea Healthcare CIC and the Board with assurance of compliance, these include:

a) IG Toolkit (DSP) Data security and protection toolkit - Annual Internal audit assessment of IG Toolkit (DSP) Data security and protection toolkit assessment.

Our organisation's declared position against the Toolkit requirements, this audit has achieved substantial assurance on each occasion.

b) Data Protection Audits – We reserve the right to do unannounced Data Protection Act audits in services across all the clinical divisions. The audits assess the risk of non-compliance with appropriate DPA principles and the effectiveness of the data protection activities with specific reference to:

- i. Data protection governance – The extent to which data protection responsibility, policies, procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.
- ii. Security of personal data – The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

The audits identify areas of good practice and areas to address. Findings from the audit are sent to the relevant managers with recommendations on how to address the identified areas of concern. Services were given a deadline to respond to the IG team to provide an update that the required changes are in place.

c) Other Audits – Battersea Healthcare CIC as part of standard audit procedures also undertake a corporate record keeping audit and clinical record keeping audit.