Intercom Trust

Lesbian, gay, bisexual and trans+ people in the South West

Registered charity 1171878

Current version approved: September 2020

Review / refresh due: September 2021

Data Quality Policy

1. Introduction

1.1. The Intercom Trust hold personal data about our clients, employees, suppliers and other individuals for a variety of relevant purposes. The Trust is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

1.2. This policy sets out how we seek to ensure accuracy of information which we store and process.

1.3. This policy applies to all personal data processed by the Intercom Trust either in hardcopy or digital copy, this includes special categories of data.

1.4. The availability of accurate and timely data is vital for the safety of the people we care for and the safe and responsible running of our organisation. This policy outlines the following procedures:

1.4.1. Procedures for ensuring data accuracy;

1.4.2. Procedures for correcting errors.

1.5. The officers responsible for the implementation of this Policy shall be the nominated the CEO, the Information Governance Lead, and other line managers. They shall also provide for it to be reconsidered and updated as necessary.

1.6. Line managers, the Information Governance Lead, and the CEO will be responsible to the Trustees for actively supervising the implementation of this policy on a day-to-day basis.

1.7. All staff must comply with this policy fully and at all times and must notify the CEO, the Information Governance Lead, and/or other line managers of any breaches of this policy.

1.8. The Trust is registered with the Information Commissioner as a holder of personal data.

2. Data accuracy procedures

2.1. We commit to ensuring that we comply with the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17 that we will "maintain securely an accurate, complete and contemporaneous record in respect of each service user, including a record of the care and treatment provided to the service user and of decisions taken in relation to the care and treatment provided";

2.2. We ensure accuracy in our data in both hardcopy and digital records by making sure all data has the following characteristics:

2.2.1. Authentic – i.e. the data is what is claims to be, has been created or sent by the person who said that they created or sent it, and that this was done at the time claimed;

2.2.2. Reliable – i.e. the data is complete, accurate, has been created close to the time of the activity it records, and has been created by individuals with direct knowledge of the event it records;

2.2.3. Integrity – i.e. the data is complete and unaltered, it is also protected from being changed or altered by unauthorised persons, any alterations are clearly marked and the person who made them can be identified;

2.2.4. Useable – i.e. the data can be located when it is required for use and its context is clear in a contemporaneous record.

2.4. The principal purpose of service user records is to record and communicate information about the individual and their care. The principal purpose of staff records is to record employment details for payroll and business planning purposes.

2.5. To fulfil these purposes, we:

2.5.1. Use standardised structures and layouts for the contents of records;

2.5.2. Ensure documentation reflects the continuum of care, that all care is person centred and that care records are viewable in chronological order;

2.5.3. Train staff on the creation and use of records and provide regular updates on good record keeping;

2.5.4. Have implemented a procedure that enables service users and staff to have easy access to their records where appropriate.

2.6. All staff who record information - whether hardcopy or electronic - have a contractual responsibility to ensure that the data is accurate and as complete as possible. This responsibility extends to any system the staff member has access.

3. Procedures for the correction of errors

3.1. In-line with national legislation, individuals have the right to have access to their personal data which we process and store. Citizens have the right to the rectification of said records in the instance that their records are inaccurate or incomplete.

3.2. Where at all possible, in the instance that we have appropriately shared that individual's records with any third-party we will inform this third-party of the rectification if appropriate.

3.3. In all cases we will respond to a request for rectification within one month. Should the request be complex this may be extended to two months, however, we will inform the individual in writing of the extension and the reasons why it is required **within one month**.

3.4. To request for their records to be rectified service users or staff should contact us with the request for rectification either verbally or in writing. If the rectification is due the record being incomplete, then the individual should also provide the supplementary information to update the record.

3.5. While we are assessing the request to rectify records we will restrict processing of the data in question.

3.6. In the instance where the rectification request is refused, the reason will be explained in full and in writing within one month of the original request having been received.

3.7. A record of all rectification requests and outcomes will be kept by the Information Governance Lead in line with timeframes outlined in the Information Governance

Alliance's Appendix 3 of the Record Management Code of Conduct for Health and Social Care 2016 (https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016).

3.8. All individuals who have their rectification request refused will be informed of their legal rights to complain to the ICO and to seek a judicial remedy.

3.9. All service users, or their legal representative, will be informed of their rights as regards their personal data, when they sign initial contracts with us.

4. Responsibilities

4.1. The CEO, as Senior Information Risk Owner, **or equivalent job role** has overall responsibility for Data Quality policies and procedures being reviewed annually.

4.2. The Deputy Director, as Information Governance Lead, has overall responsibility for staff training in data quality and for monitoring data quality throughout the organisation. They also are responsible for responding to rectification requests and recording the outcome of any request.

4.3. Every member of staff is individually responsible for the quality of data they personally record – whether on paper or electronically. Additionally, they are responsible for reporting any mistakes they do notice to the Information Governance Lead or CEO.

4.4. Staff are aware that data accuracy and security is a contractual and legislative requirement and that breach of this policy might result in disciplinary action.