Fidelity Reviews: Information Governance and Data Security

**Introduction: Who are IPS Grow and what is fidelity review?**

# What is Individual Placement and Support (IPS)?

The IPS approach involves integrating Employment Specialists into health teams, to help them become more effective at supporting individuals to access paid employment as part of their recovery plan. NHS England (NHSE) has made a commitment to expand access to IPS as part of the Long-term plan, and fidelity reviews are essential in ensuring services are delivered to a high standard and support increases in paid employment outcomes for clients.

IPS is backed by over 30 years of research and 27 successful RCTs as the most effective model in supporting people with mental health problems and/or drug and alcohol problems into paid employment1. It is also increasingly being applied to wider client groups, such as people with physical health problems.

# What is the role of IPS Grow?

IPS Grow are commissioned by NHSE to provide implementation support to help IPS services achieve high quality employment outcomes. As part of this support, we deliver fidelity reviews across England through a team of trained reviewers.

The IPS Grow team are employed by Social Finance, a not-for-profit organisation. We also use consultants employed by the Centre for Mental Health to support with the reviews.

# What is a fidelity review?

Fidelity reviews aim to help services understand what they are doing well, but also identify improvements to practice. This is all with the aim of increasing job outcomes. Services are scored against a 25-point fidelity scale ([link](http://ipsgrow.org.uk/wp-content/uploads/fidelity_review_form_uk_-_updated_dec_2018.pdf)) which covers all areas of IPS practice. The fidelity scale has been designed as a tool to support services to deliver a high-quality service. Evidence shows that services that have higher fidelity scores achieve better employment outcomes for their clients2.

The fidelity review is carried out over 2 days, and involves interviews with clinicians, senior executives, the IPS team and clients. The fidelity review will cover all 25 points of the fidelity scale.

The reviews will be carried out by IPS Grow (staff employed by Social Finance) and the Centre for Mental Health, who we subcontract to deliver these reviews.

# What happens after the fidelity review?

1 Employment Center. Available at https://ipsworks.org/wpc

2 Bond, G. R., Becker, D. R., & Drake, R. E. (2011). Measurement of Fidelity of Implementation of Evidence- Based Practices: Case Example of the IPS Fidelity Scale and Kim et al (2015). Predictive validity of the Individual Placement and Support fidelity scale (IPS-25): A replication study.

In line with international practice following each fidelity review we will be offering on site IPS

technical support to drive increased fidelity and job outcomes at each Trust. This is offered as follows:



IPS technical support is offered on site support (virtual or in person) and will focus on up to 5 fidelity items and/or operational policies. For example, this could be around performance management, supervision and service structure. It could include a range of interventions including supporting team practice strategies, field mentoring on site or in the community, coaching, training, case reviews and audits of practice.

# What kind of data do IPS Grow need to see in the review and why?

We need access to data to understand the quality of the service on offer and how closely it meets the fidelity scale. There are a number of reasons we will need access to data, these include:

* To assess and understand the quality of the work that Employment Specialists carry out with clients. This is to make sure that they are delivering a high-quality service.
* To understand how the service meets certain KPIs, such as the average time taken between a referral and first client meeting.
* To understand the governance and management processes around the service.
* To understand how the service markets itself and builds referrals and integration with clinical teams.

To help us assess the above, we will need access to the following sources of information:

* To assess quality of work with clients: client employment profiles and action plans, case notes, employer engagement logs, interviews with clients.
* To assess how KPIs are met: access to service data sheets containing information such as referral date, engagement date, job start date.
* To understand governance and management processes: interviews with managers, notes from governance meetings.
* To understand integration: interviews with clinical team members, marketing materials, case notes.

These lists are not exhaustive but give an idea of the kind of data we will need to see. A document explaining all the data that we need to see as part of the fidelity review and why will be shared separately.

This evidence is required at least 2 weeks before the date of the review, so that we can understand how your service is operating before the review.

# Will our service need to share personal data with you through the review?

Yes. Under the Data Protection Act 2018, personal data is defined as any information relating to a person (a data subject) that is either identifiable in the data, or who could be identified using other means, such as an identification number.

Some of the data listed above, such as service marketing materials, does not relate to individuals. However, service data sheets, client case notes, employment profiles and action plans all contain personal data.

As far as possible, data shared with us through the review should be anonymised. For example, service data sheets should have client names and date of birth removed. Case notes, employment profiles and action plans can have identifiable data such as names and date of birth redacted to protect client confidentiality. However, redaction is not a failsafe method, and service data sheets will still contain individual level data. For this reason, we will treat data received as personal data and protect it accordingly.

# What are our data sharing roles and responsibilities?

The IPS service provider is the Data Controller. This means that they set the means and purposes of the data collection – in other words, why and how data is collected. The data controller is responsible for getting client consent to gather, store and share data.

Social Finance (who employ IPS Grow staff) and the Centre for Mental Health (whose staff sign consultancy contracts and adhere to our terms and conditions) are Data Processors. This means that we are carrying out tasks on the data on behalf of the controller. In this case, we are using the personal data to carry out a fidelity review to assess the quality of the service provided and make recommendations for improvements.

# What does our service need to do to share data with you?

To support the safe sharing of personal data, we will sign a Data Sharing Agreement (DSA) with you. This helps all the parties be clear about their roles with regards to the data, sets out the purpose of the data sharing, covers what happens to the data at each stage and sets standards.

Your organisation will likely have a standard data sharing agreement. It can be updated to include the information outlined in this document around:

* The types of data that will be shared.
* Our roles and responsibilities.
* How we will share data.
* How we will store data.
* How it will be deleted.

We have also attached an example DSA in Annex C, which outlines the purposes of this data sharing and can be used if preferred.

We will review and sign a DSA once it has been received. The data sharing agreement should list Social Finance as data processor3.

# Will our service need to complete a DPIA (Data Protection Impact Assessment)?

A [Data Protection Impact Assessment (DPIA)](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) is a process to help you identify and minimise the data protection risks of a project. A DPIA must be undertaken for processing that is likely to result in high risk to individuals. The kind of activity that may require a DPIA include:

* Using innovative technology.
* Using profiling or special category data to decide on access to services.
* Profiling individuals on a large scale.
* Processing biometric data or genetic data.
* Matching data or combining datasets from different sources.
* Collecting personal data from a source other than the individual without providing them with a privacy notice.
* Tracking individuals’ location or behavior.
* Profiling children or targeting marketing or online services at them; or
* Processing data that might endanger the individual’s physical health or safety in the event of a security breach.

None of the above will apply to sharing data with us for a fidelity review. In addition:

* Data shared with us will be anonymised as far as possible, minimising any risk to individuals.
* Data will be stored securely within Social Finance systems (please see below for more details of our data protection policies).
* Client consent will have been received to share data for service improvement and review purposes.

We therefore do not think that sharing data with us for the purpose of a fidelity review requires a DPIA. However, the responsibility for determining whether a DPIA is needed rests with the Data Controller.

# How does our service ensure we have client consent to share data?

As the Data Controller, you will have shared a client consent form when you started working with your clients, which will provide their consent for you to gather, store and process their data to deliver the service. It will also include information about their rights with regards to the data, including the right to access, and have the data deleted.

3 Centre for Mental Health do not need to be listed as a separate processor. Their staff sign consultancy contracts and adhere to our terms and conditions when delivering these reviews.

This should also include details of how and why you may share data with Third Parties, including for the purposes of monitoring and improving service performance. A template client consent form is attached in Annex B.

As the Data Controller, you are responsible for ensuring you have client consent to share personal information with us.

# How can our service share data with you?

Our preferred method for data transfer is through a secure Office365 environment. This method has been tested on prior fidelity reviews. We outline in Annex A how you can share data through Office 365 with us.

If required, we can use alternative methods for data sharing, including through secure email (such as Egress). We need access to the files throughout the course of the review, therefore remote access to files via a screen share method will not be suitable.

# How do you store data securely?

Social Finance is Cyber Essentials Plus accredited and has built relevant ISO27001 compatible processes to ensure we meet our partners data protection requirements and recognised industry security standards, and always preserve the confidentiality, integrity and availability of personal information.

Our ICT service provider is ISO20071 accredited. Social Finance Limited is registered as a Tier 1 organisations with the ICO. Our registration number is Z1494575. We have in place both technical measures and organisational security measures that are compliant with the Data Protection Act 2018 and General Data Protection Regulation, as well as the latest ICO guidance.

# Organisational Controls

Information security responsibility sits with the Chief Information Officer. Social Finance does not meet the criteria for needing to appoint a DPO, but our CIO is a certified GDPR Practitioner. The CIO reports to the board on an ad hoc basis if required in line with our incident escalation policy. The CIO also briefs the senior management team on any related issues. Any ongoing or serious issues are discussed at the Operating Committee meeting with Business Unit Heads so that impact on all business as usual can be assessed.

# Storage of personal data

Sensitive and/or personal data processed by with Social Finance will be stored in our Office 365 environment hosted in the UK. Data stored within Office 365 which is encrypted in transit and at rest. Appropriate access policies are set that restricted to only those members of staff in the project team that are required to access the data.

Access to SharePoint is protected via multi-factor authentication methods, access policies and geographic blocks. Data Leak Prevention is configured for all systems accessing the data.

Access requests are authorised by the CIO or COO, and changes to permissions can only be applied through our ICT support provider following their ISO27001 accredited processes.

All devices accessing our system must meet our device policies, which include device encryption, up-to-date OS and software patches, current and up-to-date virus scanner. Device compliance is actively monitored.

# Transmission of personal data

Transmission of personal data to and from Social Finance systems is as specified by the data Controller and may take place via direct access to a secure Document Library in Office 365, or via encrypted file transfer method (e.g., Huddle/Egress) as so long as it is compliant with both legislation and guidelines.

# Staff Responsibilities and Training

All staff working with personal data must undertake annual data protection and information security training which includes phishing awareness. Where we process qualifying data, staff are also required to have a current DBS check within a maximum of 2 years from the project start date.

# How will data be deleted?

No personal data about clients will be placed within the fidelity report. Generalised comments may be made about clinical notes however, nothing identifiable would be produced.

2 weeks after the review has been completed (meaning the final report has been submitted to you), personal data related to the review will be deleted. Your organisation will be responsible for deleting any personal data hosted within a Microsoft Teams site or OneNote document that has been shared with us. We can provide you with an email confirmation at this point to provide assurance that all personal data has been deleted.

# Will there be a need to share personal data in technical support?

After the fidelity review, IPS Grow will offer technical support as highlighted in the first section of this document. Most of the data required through these sessions will be non-identifiable. However, in some instances we may require access to case information (with the client’s permission) in order for an IPS Grow lead to support field mentoring or case reviews, attendance at IPS meetings, clinical team meetings etc.

Access to this personal data will be covered through the Data Sharing Agreement we will sign as part of the fidelity review. Any additional personal data accessed when delivering technical support can be shared via the data sharing methods listed in Annex A. Personal data shared with us should be deleted 2 weeks after the technical support has concluded, in line with the section above.