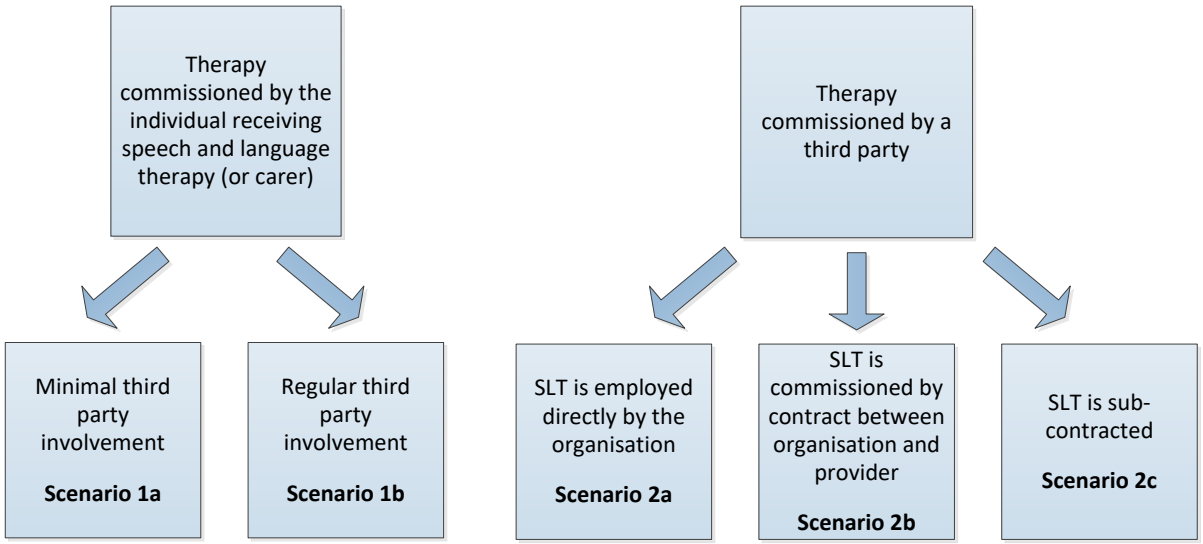
Data Protection Guidance and Scenarios for Independent Practice

About this document

This document has been developed to provide further guidance to RCSLT members working in independent practice on the implications of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. A set of scenarios have been developed to illustrate some examples of models of working in the independent sector and some key points to consider with respect to data protection.



The scenarios have been developed to guide your thoughts and prompt discussions with your colleagues about the important aspects to cover in various situations. The document should be read in conjunction with other RCSLT resources on information governance.

The RCSLT has consulted the Information Commissioner's Office (ICO) during the development of this resource. Nevertheless, it is emphasised that the information is for guidance only and does not constitute legal advice.

This document contains the following sections:

- Data processing – key points for SLTs to consider Page 2
- Therapy commissioned by the data subject Page 3
  - Scenario 1a: Minimal third party involvement Page 3
  - Scenario 1b: Regular third party involvement Page 4
- Therapy commissioned by a third party Page 5
  - Scenario 2a: SLT is employed directly by an organisation Page 6
  - Scenario 2b: SLT is commissioned via a contract between organisation and provider Page 6
  - Scenario 2c: SLT is subcontracted Page 6
- Aspects to consider when identifying the lawful basis for processing and special categories Page 7
- Aspects to consider when there is more than one data controller Page 9
- Discussion Page 10
- Sources of further information Page 10

Data Processing – key points for SLTs to consider

For each scenario, there will be elements to consider that are specific to the model of working but there are a number of key points that are applicable across all of the scenarios. These include, but are not exclusive, to the following:

- **Different data processing activities will require different lawful bases for processing.** It is very unlikely that all of the processing activities you undertake will have the same lawful basis, and you will need to consider each separately (see *Aspects to consider when identifying the lawful basis for processing and special categories*).
- **Who is the data controller for health care data?** The data controller determines the purpose and manner in which personal data is processed. As registered professionals, SLTs will usually have sole or shared data controller status for the health records they generate if they are a sole trader; otherwise the data controller is their employer or practice. The scenarios, below, are designed to help with identifying who holds data controller status, but this can vary from one situation to another. If you are the data controller, you will need to identify the activities you will carry out and the data you will need to process for each one. You should be clear about whether you are the data controller and your responsibilities before commencing processing. The ICO has also published guidance on this.
- **Inform data subjects about how their data is processed.** Data controllers are required to inform data subjects about how their data is used. Privacy notices (also known as fair processing notices) should document ways in which data will be processed (including sharing of data) and be made available to the data subject/representative. For a complete list of mandatory issues to include see the ICO guidance. The rule of thumb is that the data subject should not be surprised at how their data is being processed. You may wish to make an additional accessible privacy notice for clients with additional communication needs.
- **Consent.** Regardless of your lawful basis for processing personal data, you will need to obtain client consent for treatment. Consent is also required to share or disclose information under the common law duty of confidentiality (unless there is a legal duty to do so, or necessary to safeguard the individual or others). Please refer to the RCSLT consent guidance.
- **Ensure your policies are up to date**. Update your data security policy to provide any extra detail needed regarding data processing and refer to it in the privacy notice. This will help to keep the privacy notice concise and user friendly. Alternatively, an online privacy notice will enable layering of detail to aid clarity. Update other policies as appropriate e.g. safeguarding policies.
- **Be mindful about use of images and social media**. If making clinical photos/videos available to parents and carers, be mindful of how they may use them e.g. you may wish to specify that they must not be shared on social media. You must have consent of all participants (or parents/carers, where appropriate) to share their images with others as it would be unlikely to be necessary to the contract or provision of therapy to publish that picture. However, if you run an open day or other event that parents attend, you cannot control whether they take photos, you can only try to advise and guide (a parent taking photos would be covered by the domestic purposes exemption, whereas if you take the photo, it is part of your work purpose and must have a lawful basis under GDPR). Create/update your social media policy if appropriate.

More information about these areas is available on the RCSLT webpages.

Therapy commissioned by the data subject

Scenarios 1a and 1b outline situations where the data subject, or their representative (parent, guardian, Power of Attorney etc.) makes a personal choice to request therapy input from an independent therapist (sole trader or group practice) and is funding it directly themselves.

Scenario 1a – Therapy commissioned by the data subject with minimal third party involvement

Therapy will be carried out wholly or mainly in the client's own home or a neutral setting, though there may be occasions where a third party setting is visited on a one-off basis e.g. to carry out observation in school.

Examples

- Adult client requests home-based support for communication/eating and drinking.
- Parent requests input for child outside of school hours.
- Group therapy sessions paid for directly by clients and delivered in a "neutral" setting such as a hired room, including a school building used outside school hours (i.e. where the school's only involvement is to provide accommodation).
- Therapy commissioned directly by parents as part of a legal process, e.g. to access or challenge statutory provision for Special Educational Needs.

Issues to think about

- The SLT is the sole data controller if they are a sole trader; otherwise data controller status is held by the practice/employer.
- Agree with the data subject how data will be transferred for different purposes. For example, if you communicate with your client via email, it may be advisable to set up different mechanisms for sending confidential data, such as reports, and operational data, such as arranging therapy sessions.
- When considering the most appropriate lawful bases for processing personal data, there are a number of questions to consider. You should be aware that the lawful bases chosen will influence the individual's rights and that some bases are not available in this scenario. See *Aspects to consider when identifying the lawful basis for processing and special categories* and pp 14-17 of the RCSLT's GDPR supplementary guidance for more details.
- Contract terms and conditions to be agreed with the data subject/representative.
- Remember to think about data security practicalities when providing services at the client's home or a neutral setting. Make sure your notes are safely transported and stored whilst you are working away from your normal base, and that there is suitable privacy in the environment. Consider the advantages of electronic records and/or devices that are encrypted over paper records and diaries with respect to minimising the impact of a data breach if lost.

Scenario 1b – Therapy commissioned by the data subject with regular third party involvement

Therapy will be carried out wholly or mainly in a "third party" setting.

Examples

- Parent requests assessment/regular input for child to be carried out at school.
- Adult client requires support for communication/eating & drinking in a residential care home, day centre or similar setting.

Issues to think about

- The SLT is the sole data controller if they are a sole trader; otherwise data controller status is held by the practice/employer.
- When identifying the lawful bases for processing personal data, the same considerations as scenario 1a will be relevant. In this scenario, however, it may be that some sharing of personal data with the therapy setting is necessary for the performance of the contract you have with the data subject. If the sharing is not necessary to the contract, carefully consider why you need to share and identify suitable lawful bases to share. Think about what information will need to be exchanged with the third party on a regular basis, how this will be processed (transferred and stored), one-off situations where data may need to be shared (e.g. assessment, safeguarding).
- Considerations regarding consent and terms and conditions will be as for scenario 1a but the privacy notice may need to be enhanced to reflect the extra data processing requirements arising from the increased liaison with the third party. A direct discussion with the data subject/representative and third party may help to provide information for this and clarify expectations.
- Data security issues should be discussed at the outset. Data security can be thought of as a combination of confidentiality, integrity and availability, and the relative proportions of these will vary according to context. For instance there is often a need to balance confidentiality with the benefits of making information more available, e.g. targets on classroom displays, personal information on AAC devices, eating and drinking passports carried with the client. The use of data in this way should be explained and justified to the data subject in the privacy notice.

Therapy commissioned by a third party

Scenarios 2a-c outline situations where the therapy is funded by a third-party, not the individual themselves.

Examples:

- An organisation which has a duty to provide services for data subjects living in a certain location, for example:
    - A local authority or other public body commissions services as part of its local offer to children and young people with special educational needs (such as a mainstream SEN Service).
    - A school or local authority commissions therapy from an independent provider as a result of recommendations made by an NHS “assessment only” service.
- An organisation which has made a strategic decision to provide a service to individuals within its remit, for example:
    - A care home commissions a therapist to assess and manage the eating and drinking needs of residents.
    - A school commissions therapy to assess and treat pupils whose academic progress is causing concern (but do not qualify for input from any other source).
    - A charity offering subsidised assessments commissions a therapist to carry these out.
    - A private healthcare provider commissions therapists to carry out assessments and treatment.
- An organisation fulfilling a statutory obligation to a particular data subject, for example, a local authority commissions therapy as part of a child's Education, Health and Care Plan.
- Therapy commissioned by a local authority or other public body as part of a legal process, for example:
    - Second opinions and reports for statements of special educational need.
    - Attendance at tribunal assessments.
    - Reports and court attendance for medico-legal claims.

Scenario 2a: SLT is employed directly by an organisation

Issues to think about

- The data controller status sits with the "legal entity" employing the therapist (for example, in the case of a school, this would be the governing body). The data controller will have ultimate responsibility for the storage and management of therapy notes.
- Some organisations may not be aware of the specific requirements for processing healthcare data (e.g. who has access, appropriate retention times) and their responsibilities. Therefore, there may be a role for the SLT in supporting the data controller to ensure that the appropriate mechanisms for processing this data are in place. For instance, there will only be a limited number of people who have a valid reason to have access to the data, so it will be important to consider how this is managed.
- SLTs working in larger organisations should contact their Information Governance Department or Data Protection Officer for advice and policies.

Scenario 2b: SLT is commissioned via a contract between organisation and provider

Issues to think about

- If the organisation commissioning the service takes a role in deciding the purpose and means of processing the personal data, it is likely that there will be joint data controllership. This means that both the third party and the therapist (or their practice/employer) are both data controllers.
    - Where the SLT is joint data controller with the third party organisation, please refer to the section entitled *Aspects to consider when there is more than one data controller.*
    - Where the SLT is the sole data controller, the key considerations outlined under scenario 1b will be relevant.
- The contract terms and conditions should be agreed with the commissioner from the outset, clearly identifying the data controller.

Scenario 2c: SLT is sub-contracted

An example of this would be where a school enters into a contract with an independent therapy provider, who then sub-contracts out some of the work to a separate independent therapist in order to meet demand.

Issues to think about

- There are potentially three data controllers in this scenario: the organisation funding the speech and language therapy, the therapy provider and the sub-contracted therapist (or their practice/employer).
- As in scenario 2b, there needs to be a written agreement defining how the data controller responsibilities will be apportioned in order to protect the rights of data subjects, as well as an agreement on what data will be shared and why. Please refer to the section entitled *Aspects to consider when there is more than one data controller.*
- The sub-contracted SLT should carefully review and agree the contract terms and conditions with the intermediate provider, with input from the commissioner.

Aspects to consider when identifying the lawful basis for processing and special categories

Data protection legislation requires that the lawful basis for processing personal data is identified and clearly documented. It is the responsibility of the data controller to establish which lawful basis under article 6 of the GDPR applies to each of their processing activities. There is also a requirement to specify a further condition for processing "special category data" under Article 9 of the GDPR. Further information about this is available in the RCSLT's GDPR supplementary guidance.

Set out below are some aspects to consider when identifying the most appropriate lawful basis for both clinical and non-clinical data processing activities.

Clinical data processing activities

- If there is a direct contractual relationship between the SLT and the client (e.g. scenarios 1a and 1b), "contractual" may be an appropriate lawful basis for processing.
- Where an independent provider is contracted to provide an NHS service (e.g. scenarios 2b and 2c), "task in the public interest" may be an appropriate lawful basis, as the SLT would in effect be helping the NHS discharge its functions.
- If employed by a public sector body (e.g. scenario 2a), then "legitimate interests" cannot be used as a lawful basis, although this is allowable in private practice.
- As a rule, "consent" is not often the most suitable lawful basis for the processing of clinical data, as the work could not be undertaken without consent (and therefore a genuine choice cannot be offered)[1]. However, there are certain circumstances where consent relating to clinical data may apply, for instance, if a third party requests a specific piece of information but you do not judge the sharing of this to be necessary from a clinical point of view. In this case it may be valid to seek consent from the data subject for the sharing of that particular information. An example of this would be if an OFSTED inspector asks to see information about a specific child during an inspection, as the disclosure of this would not be clinically relevant.
- A request to share data for safeguarding purposes would be covered by "legal obligation".

[1] The GDPR defines high standards for consent. Consent under the GDPR must be freely given, specific, informed, unambiguous and involve a clear affirmative action. If consent does not meet these four criteria it is not valid for the purpose of the GDPR. Under GDPR, consent must offer the individuals genuine choice and control over the processing of their personal data. Consent must also be specific and 'granular' (i.e. separate consent is required for separate processing activities) and should be reviewed regularly. Furthermore, if using consent as the lawful basis for processing, the individual has the right to withdraw consent at any time.

For these reasons, 'consent' is not always the most appropriate lawful basis for processing personal data for direct care, and others should be considered. Consent may, however, be an appropriate lawful basis for purposes other than direct care.

It is important to note that there are a number of pieces of legislation and policy governing consent for activities linked to healthcare. **Consent under GDPR differs from patient consent to treatment and consent to share confidential information under the common law duty of confidentiality.** For further information, please refer to the RCSLT guidance on confidentiality and consent. The Information Commissioner's Office has also published detailed guidance on consent.

Non-clinical data processing activities

- Identify the lawful basis for processing data relating to your other business activities such as finance and marketing. The lawful basis may vary for each activity. For example, the statutory requirement to hold financial data for tax reporting purposes would be covered by "legal obligation".
- If you are intending to use client data for marketing purposes (e.g. offering additional group sessions, training etc.), then this is a separate data processing activity for which "consent" would be an appropriate lawful basis. Check that the wording of your documentation makes it clear that consent for marketing is separate and distinct from consent for therapy.
- Further, explicit consent must be obtained if the commissioner (e.g. school) wishes to use the personal information of data subjects on your caseload for marketing purposes (e.g. to offer optional school holiday groups funded by parents).

Aspects to consider when there is more than one data controller

In scenarios where the SLT is the joint data controller (e.g. 2b and 2c), it is important to be clear about how the data controller responsibilities will be apportioned, including what the roles of both parties are during and at the end of the contract. Outlined below are some key considerations:

- A written agreement setting out the data controller responsibilities should be set up at an early stage, preferably before provision begins, and then reviewed regularly. This agreement will help to protect data subjects and reduce the risk of complaints and disputes about the way data is processed. The agreement should also define what data is to be shared between controllers, why, and which lawful bases are relied upon for that sharing.
- There is no set formula or template for this, providing that all the data controller responsibilities and data subject rights are covered (how will data be stored, how will subject access requests be handled etc.).
- Think about who needs to be involved in drawing up the agreement, including the data protection officer in the organisation(s) and any other people that can provide information on what needs to be included, such as the special educational needs co-ordinator.
- The above agreement can form part of the contract between the organisations. If the organisation commissioning the service does not provide a contract, be prepared to initiate a conversation about this and you may wish to produce a draft agreement for discussion. Some organisations may not be aware of the specific requirements and their responsibilities as a joint controller for processing healthcare data.
- If the contractual department of a larger organisation (e.g. local authority or other public body) is not forthcoming, or include requirements in the contract that are in conflict with professional obligations (e.g. stipulating that data must be destroyed or returned when the contract ends), it is worth involving the information governance department directly as they will have a more detailed understanding of data processing requirements.
- Data should only be shared on a “need to know” basis. One of the principles of GDPR is that information is not to be processed unnecessarily, so, for example, a school asking for blanket access to SLT notes would need to justify why this is required. Data controllers must ensure they disclose only the relevant information to each other.
- Make sure privacy notices cover any partnership working and that it is clear to the data subject what is happening to their data and who to contact to exercise their rights.
- If an intermediate provider or the organisation funding the therapy (scenarios 2a – 2c) request that you to use their system for recording client notes, you need to be satisfied that the system meets professional requirements for record keeping. In return, they should check that you have adequate data protection knowledge before allowing you to access their systems.

Discussion

Having considered the scenarios above, think about which of the above scenarios most closely applies to your practice:

1. Are there any aspects that you need to consider or explore further?

2. If so, what steps do you think you need to take next?

3. Are you aware of the resources available to help you?

Sources of further information

- HCPC Confidentiality - Guidance for Registrants
- ICO FAQs for small health sector bodies
- ICO Guidance on Data Controllers and Processors
- ICO *Data Sharing Code of Practice* (including checklists) can be found at www.ico.org.uk
- ICO Data Protection Self Assessment
- RCSLT Guidance on Confidentiality
- The Wales Accord for Sharing Personal Information provides data sharing templates aimed at partnerships providing public services. WASPI reflects the ICO Data Sharing Code and is being updated to reflect GDPR.