Information Sharing and Privacy Protocol

|  |  |  |
| --- | --- | --- |
| Policy Title / Reference | Author | Owner |
| Information Sharing and Privacy Protocol | Emma Cooper, Cluster DPO (Kafico) | Practice Manager |

|  |  |  |
| --- | --- | --- |
| Version | Revision author | Version comments |
| 1 | Emma Cooper, Kafico Ltd | Jan 18 New Draft |
| 1.1 | Emma Cooper. Kafico Ltd | Jan 2019 Replaced 1998 DPA with 2018 Act. Replaced GDPR with “data protection legislation”. |
| 1.2 | Emma Cooper Kafico Ltd | Japan now approved for EU data transfers. Added to list in appendix. |

Contents

[2. Scope 2](#_Toc7421090)

[3. Definitions 3](#_Toc7421091)

[4. Introduction 3](#_Toc7421092)

[5. Statutory Mandatory Framework 3](#_Toc7421093)

[6. Accountable Parties 4](#_Toc7421094)

[7. What Information is Covered? 4](#_Toc7421095)

[8. Transparency 5](#_Toc7421096)

[9. Considerations when Sharing Personal Confidential Information 6](#_Toc7421097)

[10. Sharing Information with Third Parties 7](#_Toc7421098)

[11. Maintaining a Secure Operational Environment (SOE) 7](#_Toc7421099)

[12. Telephone Enquiries 7](#_Toc7421100)

[13. Requests for Personal Confidential Information by the Patient, the Police or the Media. 8](#_Toc7421101)

[14. Disclosure of Personal Confidential Information to Other Employees 9](#_Toc7421102)

[15. Carelessness 9](#_Toc7421103)

[16. Use of Internal and External Post 9](#_Toc7421104)

[17. Faxing confidential information 10](#_Toc7421105)

[18. E-mailing Personal Confidential Data 10](#_Toc7421106)

[19. Paper Records 10](#_Toc7421107)

[20. Mobile devices 11](#_Toc7421108)

[21. Disposal of Personal Confidential Information 11](#_Toc7421109)

[22. Confidentiality of Passwords 11](#_Toc7421110)

[23. Working remotely 12](#_Toc7421111)

[24. Abuse of Privilege 12](#_Toc7421112)

[25. Information Incidents 12](#_Toc7421113)

[26. Associated Protocols 13](#_Toc7421114)

[27. Audit Schedule 13](#_Toc7421115)

[28. Review 13](#_Toc7421116)

[Appendix A: Sharing Scenarios 14](#_Toc7421117)

[Appendix B Non-Standard Information Sharing Template 16](#_Toc7421118)

[Appendix C Transfers of Data outside of the UK 20](#_Toc7421119)

[Appendix D Contract IG Compliance Checklist 22](#_Toc7421120)

# Scope

This protocol has been drafted for use by customers of Kafico Ltd across Norfolk and Waveney.

At the time of writing and unless alternative protocols have been adopted locally, the protocol applies to;

|  |  |  |
| --- | --- | --- |
| Acle Medical Partnership | Boughton Doctors Surgery | Hellesdon Medical Practice |
| Beccles Medical Centre | Bridge Street Surgery | Holt Medical Practice |
| Birchwood Surgery | Cromer Group Practice | Feltwell Surgery |
| Blofield Surgery | St Clement's Surgery | Great Massingham and Docking Surgeries |
| The Brundall Medical Centre | Castle Partnership | The Harleston Medical Practice |
| Coltishall Medical Practice | The Burnhams Surgery | Heacham Group Practice |
| Campingland Surgery | Drayton Surgery | St John's Surgery |
| Hoveton & Wroxham Medical Centre | Roundwell Medical Centre | Staithe Surgery |
| Ludham Surgery | Paston Surgery | Thorpewood Surgery |
| The Market Surgery | Prospect Medical Practice | Upwell Health Centre and Welle Ltd |
| Howdale Surgery | Sheringham Medical Practice | Watlington Medical Centre |
| Litcham Health Centre | Southgate and Wootton’s | Wells Health Centre |
| Mundesley Medical Centre | St James Medical Practice | St Stephen’s Gate |
| Manor Farm Medical Centre | The Fakenham Medical Practice | Plowright Medical Centre |
| Grimston Medical Centre |  |  |

# Definitions

**Personal Confidential Information** This term is intended to cover information captured by the Data Protection Act 2018 / GDPR (identifiable information about the living), information covered by the Common Law Duty of Confidence / Tort of Misuse of Private Information and finally, information covered by Article 8 European Convention for Human Rights.

# Introduction

Privacy is a concept that emerges from a complex area of law. The three key elements of privacy arise from the Common Law Duty of Confidence / Tort of Misuse of Private Information, Article 8 European Convention of Human Rights (Right to Privacy) and the Data Protection Act 2018 / General Data Protection Regulations (GDPR). This protocol intends to support staff in navigating this framework and encourage lawful, secure and appropriate information sharing.

# Statutory Mandatory Framework

**Data Protection Act 2018 / General Data Protection Regulations (GDPR**

This legislation protects Personal Data (information which identifies or could identify a living individual).

**Common Law Duty of Confidence / Tort of Misuse of Private Information**

This common law protects information which a ‘reasonable person’ would expect to remain private. This might include financial / contract information or information about the deceased.

**Article 8 European Convention of Human Rights (Right to Privacy)**

This inherent human right determines that citizens have a right to have their information and family life protected from arbitrary interference from the state – i.e. public bodies or those working on behalf of public bodies.

# Accountable Parties

See Information Governance Policy for key roles.

All staff, whether management or administrative, who create, receive and use Personal Confidential Information have responsibilities to ensure lawful, secure and appropriate information sharing. Employees have a contractual and legal obligation to read and comply with all company policies and to attend mandatory training to support the appropriate management of information.

# What Information is Covered?

Information may be held on paper, USB sticks, computer file or printout, laptops, tablets, mobile phones or even heard by word of mouth or telephone.

Personal Confidential Information includes information that contains the following;

Direct identifiers:

|  |  |
| --- | --- |
| * [Name](https://en.wikipedia.org/wiki/Full_name) | * [Home address](https://en.wikipedia.org/wiki/Address_(geography)) |
| * [Email address](https://en.wikipedia.org/wiki/Email_address) | * [National identification](https://en.wikipedia.org/wiki/National_identification_number) / NHS Number |
| * [Passport](https://en.wikipedia.org/wiki/Passport) number | * [IP address](https://en.wikipedia.org/wiki/IP_address) |
| * [Digital identity](https://en.wikipedia.org/wiki/Digital_identity) | [Date of birth](https://en.wikipedia.org/wiki/Date_of_birth) |
| * [Birthplace](https://en.wikipedia.org/wiki/Birthplace) | * [Login](https://en.wikipedia.org/wiki/User_(computing)), screen name, [nickname](https://en.wikipedia.org/wiki/Nickname), or [handle](https://en.wikipedia.org/wiki/Pseudonym) |
| * [Telephone number](https://en.wikipedia.org/wiki/Telephone_number) |  |

Indirect identifiers:

|  |  |
| --- | --- |
| * Country, state, [postcode](https://en.wikipedia.org/wiki/Postcode) | * Age (particularly if extreme i.e. very old) |
| * [Gender](https://en.wikipedia.org/wiki/Gender) or race | * Name of the school they attend or workplace |
| * Grades, salary, or job position | * [Criminal record](https://en.wikipedia.org/wiki/Criminal_record) |
| * Health records | * Web Cookie / IP address |

Additionally, the term includes information that may ***not***identify the individual but the individual has requested or would reasonably be expected that it remain private and therefore creates a duty of confidentiality.

Some information is more sensitive and requires additional care and requires a specific lawful basis to handle it. This is because, if accessed by an unauthorised individual, this type of information has the potential to cause damage or distress to the data subject.

|  |  |
| --- | --- |
| * racial or ethnic origin | * political opinions |
| * political opinions | * physical or mental health or condition |
| * religious or similar beliefs | * sexual life |
| * trade union membership | * Commission (actual or alleged) or proceedings for an offence |
| * Biometrics such as fingerprints |  |

Non-person-identifiable information can also be considered confidential. For example, confidential business information such as financial reports; and commercially sensitive information such as contracts, trade secrets, procurement information. This information should also be treated with care.

# Transparency

Any activity that involves processing Personal Confidential Information should involve consideration of how individuals might be made aware and have an opportunity to object

The information to be supplied must be;

* concise, transparent, intelligible and easily accessible;
* written in clear and plain language, particularly if addressed to a child; and
* free of charge

These ‘Privacy Notices’ are discussed in more detail in the Information Access and Rights Protocol.

# Considerations when Sharing Personal Confidential Information

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check there is a legal basis for disclosure before releasing it. This will be provided in the Information Sharing Agreement or Protocol. A copy should be made available to your department by the Information Governance Lead or DPO.

Where possible, information should be de-identified prior to disclosure. For de-identification, the above direct and indirect identifiers of the individual are removed. The practice may retain a code or other means of record identification to allow de-identified information to be re-identified and this must be kept secure.

Where a code is available to The practice or someone outside of The practice to enable re-identification – such as the NHS No, the data is classified as pseudonymized but is still Personal Confidential Information and should be treated as such.

Where **all possibilities** of re-identifying a record to a service user has been removed then the data would be considered fully anonymised and is no longer Personal Confidential Information.

When personal information is being shared routinely between The practice and other organisations – the Information Sharing Protocols or Agreements mentioned above will support your sharing decisions and identify best practice.

When you are required to share personal information for a ‘one off’ purpose, you should consider the potential benefits and risks, either to individuals or society, of sharing the data. You should also assess the likely results of not sharing the data and apply common sense.

See **Appendix A Data Sharing Scenarios** and **Appendix B Non-Standard Information Sharing Template** for more information.

Do not send or take any Personal Confidential Information out of the EEA unless the country is listed in **Appendix C Transfers of Data outside of the UK** or the transfer forms part of an established Data Sharing document.

With any request to share Personal or Sensitive Personal Confidential Information outside of usual practice, always speak with the Caldicott Guardian or Data Protection Officer to confirm the approach.

# Sharing Information with Third Parties

All routine sharing of Personal Confidential Information should be covered by an Information Sharing document.

When the sharing is between two Data Controllers for example the practice and a hospital, there should an Information Sharing Agreement in place.

Where the sharing is between the The practice and an organisation processing Personal Confidential Information on its behalf, there should be a Processing contract in place that meets with the requirements of GDPR Article 28 and s 59 DPA 2018. See **Appendix D.**

Where a third party is not processing Personal Confidential Information on The practice’s behalf but may come in to contact with such data incidentally, they must have signed a confidentiality agreement.

# Maintaining a Secure Operational Environment (SOE)

Secure operational environment exists when there is either a secure physical location or an agreed set of administration arrangements in place within the organisation to ensure Personal Confidential Information is handled and shared safely and securely.

It is a safeguard for privacy for all the stakeholders of The practice. Any members of staff handling Personal Confidential Information, whether paper based or electronic must adhere to the SOE principles. The guidelines below identify how The practice maintains a SOE and so it is crucial that all staff are aware of and comply with this Procedure.

# Telephone Enquiries

A patient or member of the public may telephone The practice, for example to report a technical problem or to access some information, or a health and social care provider may call in to check on the status of a patient they referred.

Some people attempt to gain information from organisations illegally by deception.

This practice is known as Voice Phishing or “blagging” and is part of an illegal trade in Personal Confidential Information. An individual with a legitimate request will be open about their activity and will not need to resort to Voice Phishing.

You should not disclose any information unless you are sure they are the person they say they are and need access to the information as part of their job role. If in any doubt, do not disclose the information and speak to the Information Governance Lead or Data Protection Officer.

If a request for personal information is made by telephone, always satisfy yourself as to the identity of the caller by;

|  |  |
| --- | --- |
| * confirming the identity of the individual | * if in doubt as to whether the information should be disclosed tell the caller you will call them back and take advice from your manager |
| * confirm the reason for the request and only share the minimum necessary information, particularly information related to health | * ensure you keep a record of your name, date/time of disclosure, the reason for it, who authorised it and the contact details of the recipient |
|  |  |

Remember that even the fact that an individual is known to the practice is confidential. If in doubt consult the Caldicott Guardian or Data Protection Officer.

# Requests for Personal Confidential Information by the Patient, the Police or the Media.

Please refer to the Information Access and Rights Protocol.

# Disclosure of Personal Confidential Information to Other Employees

In line with the ‘Need to know’ principle, Personal Confidential Information should only be released to individuals that have a genuine, identified business need.

Don’t be coerced into giving out Personal Confidential Information. If in doubt, check with a senior member of staff.

# Carelessness

Do not talk about patients or staff in public places or where you can be overheard

Do not leave any medical or staff records or confidential information lying around unattended

Make sure that any computer screens, or other displays of confidential information i.e. whiteboards, cannot be seen by anyone who does not need to know. Ensure that screens are locked when away from your desk.

# Use of Internal and External Post

Maintain a clear desk policy and undertake regular checks where possible to identify errors or potential breaches.

Staff should not copy or amend existing letters – use a fresh template to avoid errors.

High volume or bulky material must only be transported in approved boxes and never in dustbin sacks or other containers and must be locked away until collected by an approved carrier.

Personal Confidential Information should always be labelled as Private & Confidential on the envelope and letters should be addressed to an individual rather than a team where possible.

Always provide a return address and ensure the packaging is robust.

# Faxing confidential information

It is The practice’s policy to avoid the use of faxes for sharing of Personal Confidential Information because of the large number of information incidents where faxes have been identified as a problem. In the event a fax **must** be used then only use the minimum amount of information necessary and follow this procedure;

* Faxes should be addressed to named recipients and be marked as confidential.
* Use the considerations for sharing under section 4.
* Review the report sheet to confirm that the transmission was OK
* Ensure the fax is located is a secure area, accessed by minimum number of individuals
* Used locked print where available

# E-mailing Personal Confidential Data

Personal Confidential Information must be sent using a secure email service such as Nhs.net

If, for any reason this is not possible, it should be sent in a password protected spreadsheet, with the password being given to the recipient separately by phone.

Always double check you are sending the email to the correct person/s.

Regularly check / update your distribution list to ensure copies are not sent to staff who have left, moved to another service or no longer require the information

Where possible, telephone the recipient of the e-mail to let them know you are going to send Personal Identifiable Information

When emailing information to several members of the public always use bcc so that their email addresses are not visible to one another.

# Paper Records

When printing Personal Confidential Information use the ‘locked print’ facility. Departments that are printing any Personal Confidential Information should have a limited access printer

Never leave Personal Confidential Information on the printer / photocopier

If you find unclaimed personal information in the printer / photocopier, you must complete an information incident form.

Clear your desk at the end of each day, keeping all portable records containing Personal Confidential Information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised

Paper records must always be kept locked away when unattended.

# Mobile devices

Mobile devices include but are not limited to:

|  |  |
| --- | --- |
| * Laptops | * PDA’s |
| * USB Memory Sticks | * Digital Cameras |
| * CD-R’s | * Tablet PCs |
| * DVD-R’s | * Multi-Function Mobile Devices (Smart Phones, Blackberry) |

No removable media containing Personal Confidential Information should be removed from [insert practice name] premises unless agreed by your team manager. Personal Confidential Information should only be stored off the practice shared network i.e. on your personal computer if it is absolutely necessary and should be agreed by your team manager.

# Disposal of Personal Confidential Information

Please refer to Creation, Storage and Destruction Procedure.

# Confidentiality of Passwords

Passwords are confidential and must not be shared

All attempts to bypass the Information Security Policy of The practice by using another person’s password, may result in disciplinary procedures or dismissal.

# Working remotely

Taking home / removing paper documents that contain Personal Confidential Information from the practice premises is discouraged. If necessary, they must be kept out of sight whilst being transported or worked upon.

Staff must ensure that their remote working practice complies with The practice policies and procedures.

Staff are responsible for keeping Personal Confidential Information secure and confidential whilst working remotely, including preventing incidental access by friends / family.

All information on mobile devices must be transferred to the network as soon as possible and the information then erased from the mobile device.

# Abuse of Privilege

All practice staff are strictly forbidden to access their own Personal Confidential Information unless specifically authorised to do so.

Staff are forbidden to access any personal information relating to public figures, colleagues, friends or relatives unless they have a legitimate reason to do so as part of their employment responsibilities.

Such activity would be a breach of the Computer Misuse Act 1990 and / or Data Protection legislation.

If you wish to request a copy of your Personal Confidential Information refer to Information Access and Rights Procedure.

# Information Incidents

Any suspected or actual incidents involving Personal Confidential Information must be reported immediately in line with the Information Incident Protocol.

# Associated Protocols

This policy should be read in conjunction with;

* Risk Management Policy
* Change Management Policy
* Information Governance Policy
* Information Rights and Access Protocol
* Information Lifecycle and Data Quality Protocol
* Information / Cyber Security Protocol
* Information Incident Protocol
* Information Risk and Audit Protocol
* Data Protection Impact Assessment Protocol
* Freedom of Information Protocol

# Audit Schedule

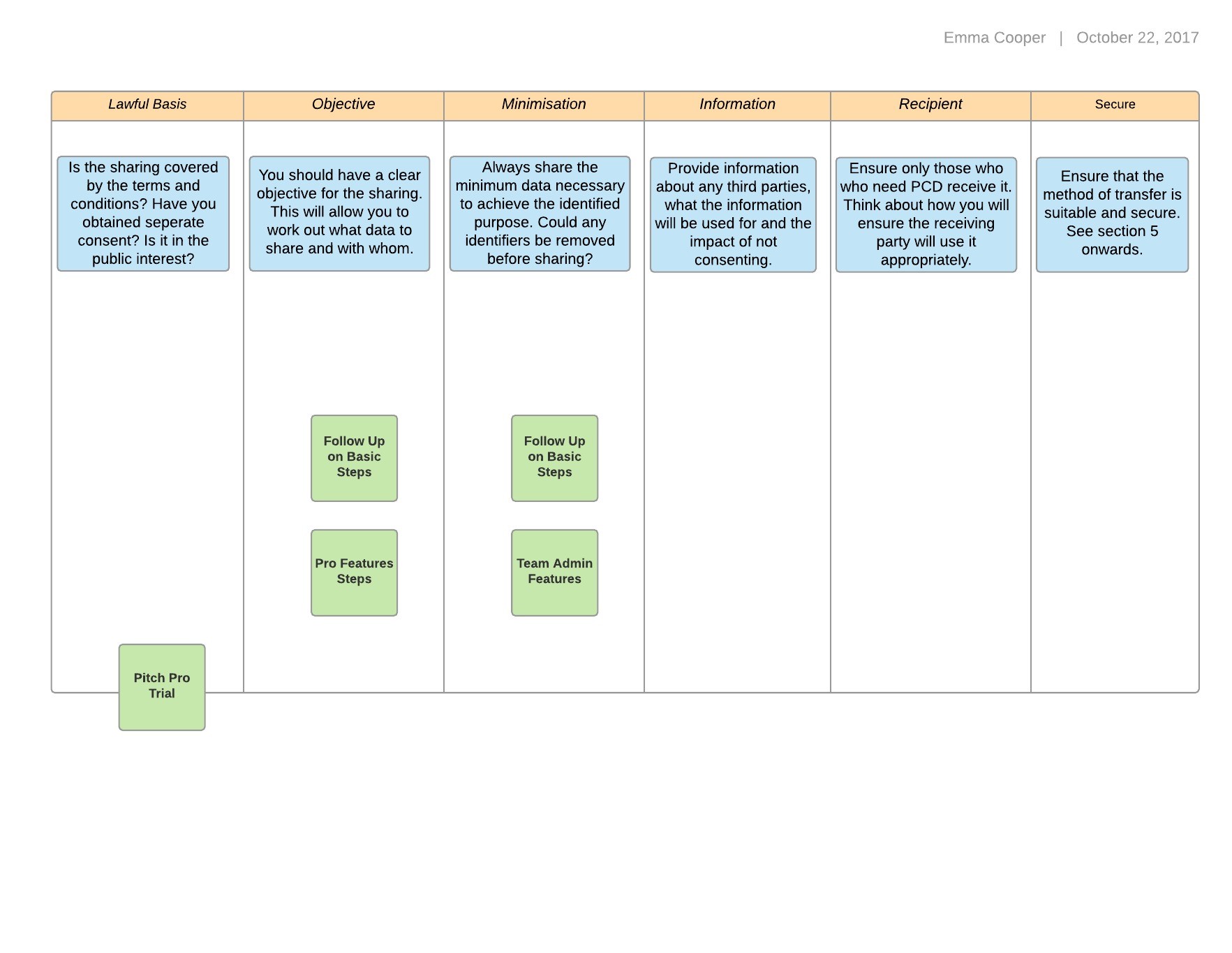
Compliance with this protocol will be audited and the results fed into the Plan, Do, Check, Act Cycle described in the Information Risk and Audit Protocol.

# Review

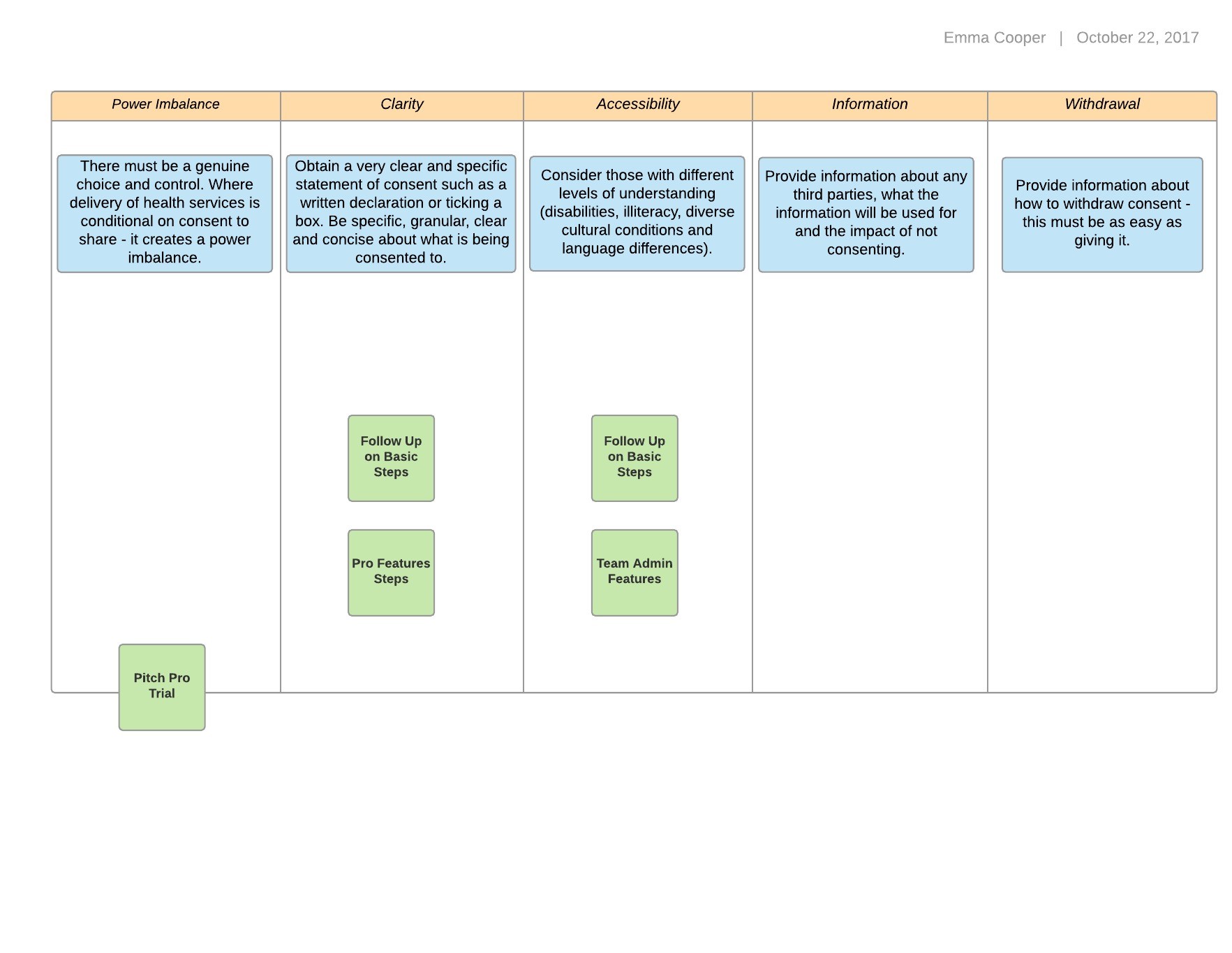
This protocol will be reviewed every year or sooner where necessary.

# Appendix A: Sharing Scenarios

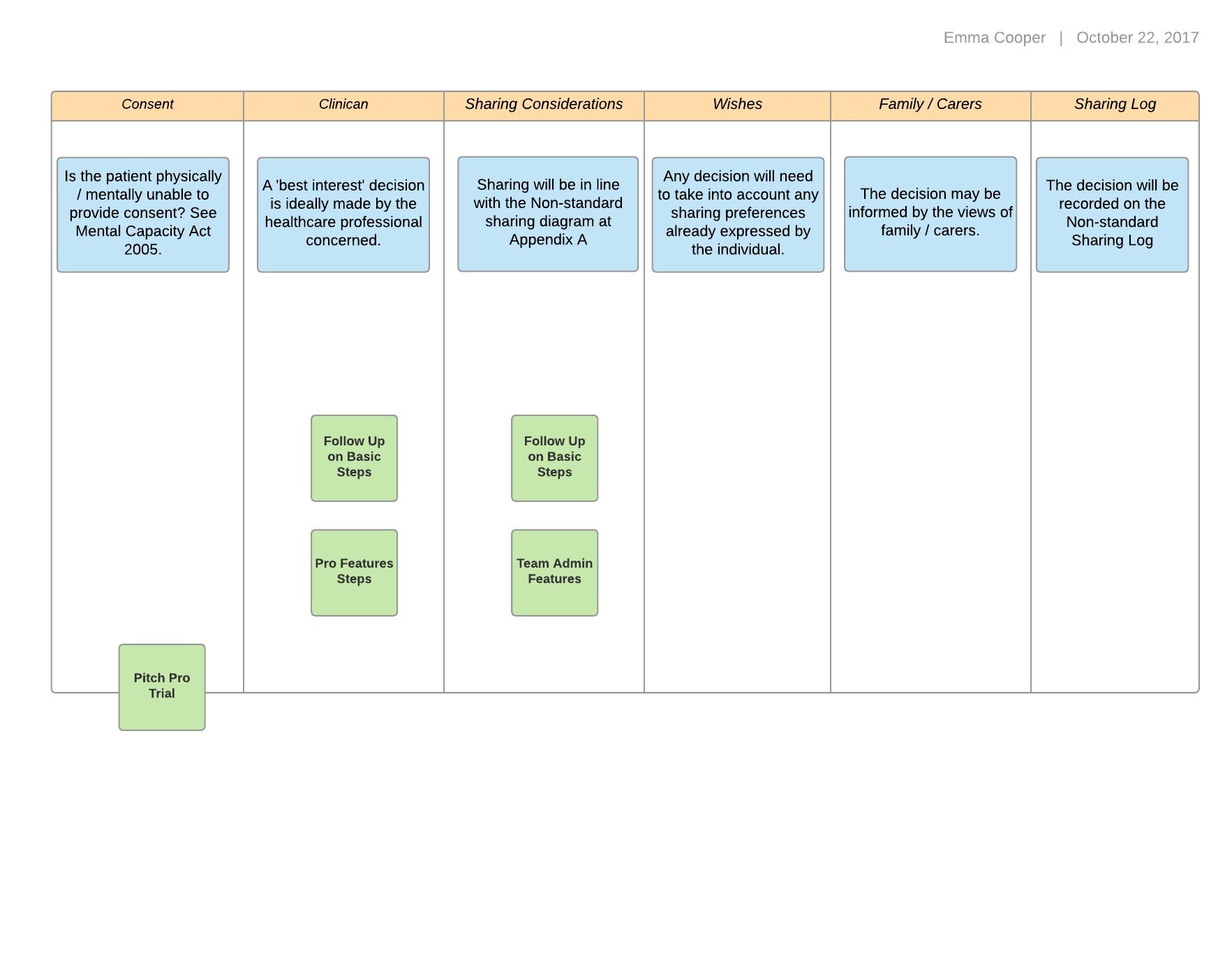
Non-Standard Sharing of Personal Confidential Information



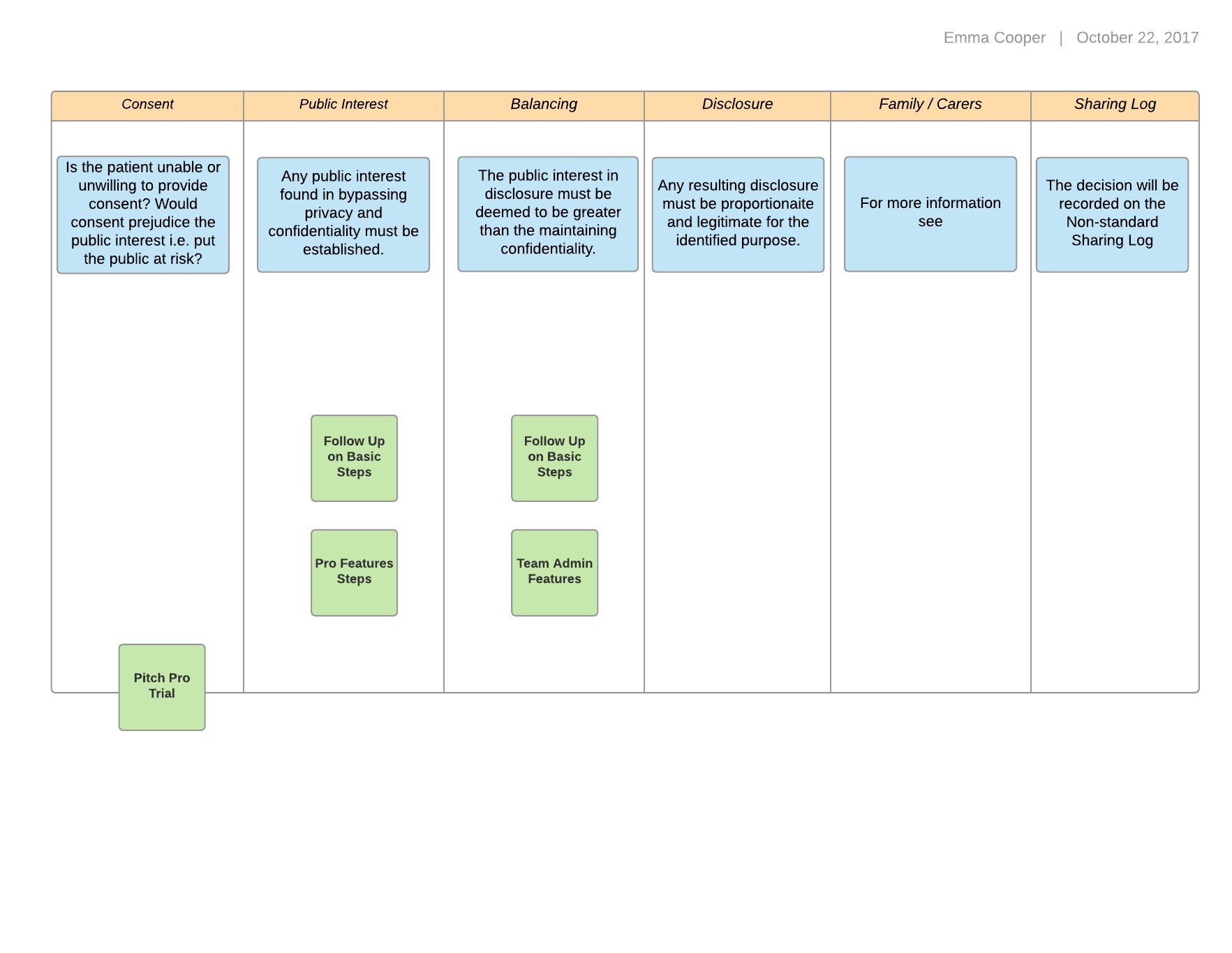
Obtaining Consent to Process / Share Personal Confidential Information



Sharing Personal Confidential Information in the best interests of the Individual



Sharing Personal Confidential Information in the public interest



# Appendix B Non-Standard Information Sharing Template

|  |  |
| --- | --- |
| What are the details of the sharing request (no personal data)? |  |
| Do you have a clear objective for disclosure? This will allow you to determine what needs to be shared and with whom. |  |
| What is the lawful basis under Data Protection legislation?  For example, public interest, court order, delivery of healthcare. |  |
| On what basis is the duty of confidentiality set aside?  For example, public interest, court order, the individually ‘reasonably expects’ such a disclosure |  |
| Does the disclosure represent a lawful interference with the individuals’ rights to privacy under the European Convention of Human Rights?  For example, it is lawful, it is in order to protect health and morals. |  |
| Identify the public interest factors for disclosure that outweigh the public interest in maintaining confidentiality.  For example, public interest in protecting individuals from harm, public interest in observing the rights of individuals to access their information, the public interest in prevention and detection of crime. |  |
| If the request is a subject access request made on or by the individual, please consult the Information Access and Rights Protocol. |  |
| Has a review been carried out to ensure that the minimum necessary data has been requested for the lawful purpose? Could any identifiers be removed? |  |
| Consider whether the individual has or will be notified about the disclosure. If this would prejudice the purpose in some way – document it here. |  |
| Consider the specific individual that the information should be disclosed to and ensure there is a ‘need to know’ |  |
| Has a review been carried out to ensure that the information being requested is legitimate and necessary for the lawful purpose? |  |
| Consider the methods for sharing information in terms of their security and safeguards in place. |  |
| Outcome |  |
| **Sharing to Safeguard Children** | |
| Which section of the Children Act is the request for information being made to support? i.e. s17, s47 |  |
| Does the requestor **genuinely and reasonably** believe that it is desirable to share information to protect children? |  |
| Has consent been obtained and if not, would doing so prejudice the lawful purpose? |  |
| Would the sharing of information be in the public interest? |  |
| Is the Common Law Duty of Confidentiality lawfully set aside because the information is necessary to discharge a legal duty under Children Act? |  |
| Is it believed that sharing the information would support protection of the individuals Article 3 right to be protected from ‘*torture or … inhuman or degrading treatment or punishment’?* |  |
| Would sharing the information support protection of the individuals Article 2 right to life*?* |  |
| Is it believed that sharing the information would represent a **lawful and proportionate** interference with the child’s Article 8(1) right to privacy? |  |
| Is it believed that sharing the information would represent a lawful and proportionate interference with **other individuals’** Article 8(1) right to privacy? |  |
| Are both / all parties signatories to a Multi-Agency Safeguarding Information Sharing Agreement? |  |
| Has a review been carried out to ensure that the minimum necessary data has been requested for the lawful purpose? |  |
| Has a review been carried out to ensure that the information being requested is legitimate and necessary for the lawful purpose? |  |
| Outcome |  |

# 

# Appendix C Transfers of Data outside of the UK

The EEA countries where data may be transferred without additional assurances are:

|  |  |  |
| --- | --- | --- |
| Austria Belgium Bulgaria Croatia Cyprus Czech Republic Denmark Estonia Finland France | Germany Greece Hungary Iceland Ireland Italy Latvia Liechtenstein Lithuania Luxembourg | Malta Netherlands Norway  Poland Portugal Romania Slovakia Slovenia Spain Sweden United Kingdom |

The following also have an adequate level of protection for personal data

|  |  |  |
| --- | --- | --- |
| Andorra Argentina Faroe Islands | Guernsey Isle of Man Israel Japan Jersey | New Zealand Switzerland Uruguay |

# Appendix D Contract IG Compliance Checklist

In line with the requirements of GDPR Article 28 and s 59 DPA 2018, this contract allows [insert practice name] to review the contracts in place with Data Processors and ensure they are compliant.

This checklist serves as a first part of the process towards confirming that a contract contains the relevant terms and conditions to allocate Data Protection responsibility and to ensure that appropriate controls are in place to protect Personal Confidential Information

In the Data Protection Act 2018, the Data Processor acts only on the instruction of the Data Controller and this MUST be under a legally enforceable contract.

|  |  |
| --- | --- |
| Contract/Supplier Name: |  |
| Synopsis of use of information and types of information used: |  |
| Date Checklist Completed: |  |
| Senior Responsible Owner: |  |

| **Required clause/areas covered by contract** | **Included y/n/NA** | **Notes/Comments** |
| --- | --- | --- |
| If possible, please attach or provide a map of data flows, i.e. where information will travel from and to, and what the information might contain |  |  |
| Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect personal data including storage and transmission of data, business continuity, staff training, auditing, access control and Cyber security? |  |  |
| Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller? |  |  |
| Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller? |  |  |
| Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law and in those cases will notify the Controller? |  |  |
| Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with third party unless required to do so by law? |  |  |
| Does the contract require the Processor to assist the Controller to respond to requests for exercising the data subject's rights i.e. access to information, correction of errors? |  |  |
| Does the contract require the Processor to assist the Controller in reporting information incidents promptly including where it might be required to contact the data subject? |  |  |
| Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction? |  |  |
| Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller? |  |  |
| Does the contract state that the Processor will immediately inform the Controller if the Processor is instructed to undertake unlawful activity? |  |  |
| Does the contract identify that, if a processor infringes the contract by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing? |  |  |