Sensitive Information Map, PIA and Risk Assessment

Privacy Impact Analysis (PIA)

Why we are performing a PIA
We are carrying out a PIA to help us to minimise the risks of data processing. We will draw upon the results of other risk assessment in the Information Governance series of templates. In particular we want to make sure that personal information is not:

- Inaccurate, insufficient or out of date
- Excessive or irrelevant
- Kept for too long
- Disclosed to those who the person it is about does not want to
- have it
- Used in ways that are unacceptable to or unexpected by the
- person it is about
- Kept in a way that is insecure

This PIA will be reviewed each year and also if we use new technology or process personal data in a new and different way than we do now. This is the structure of our Privacy Impact Analysis in this document:

- The information flows are detailed below in the Information Map, and the Outgoing and Incoming Information flows
- The data privacy and related risks are assessed in the Business Impact Analysis (M 217N)
- The privacy solutions, or ways that privacy risks can be reduced to a minimum are found in the Business Impact Analysis (M 217N) and in the Information Security section of the Information Governance Procedures (M 217C)
- Consultation and training with the team happens at [an iComply practice meeting once a year]
- The PIA outcomes are considered at the end of this document

Information Map

About our data and where it is held	
The personal data types we hold are	[Employment records, marketing information such as email addresses, home addresses, other]. We share personal data with [our accountants to process salaries, other]
How we hold personal data	Personal data is held in hard copy, securely at the practice and in electronic format at the practice and online
How we collect personal data	We collect personal data directly from team members or patients by [phone, in person, by email, using online forms, from referrals, other]
The special category data types we hold are	[Patient health records, team health records, criminal disclosure details, photographs, videos, other]. We share special category data with [other healthcare practitioners or secondary health care providers for the purpose of referring patients for health care services, other]
How we hold special category data	Special category data is held in hard copy, securely at the practice and in electronic format at the practice and online
How we collect special category data	We collect special category data directly from team members or patients, by [phone, in person, by email, using online forms, from referrals, other]

Where we keep digital data	[On practice computer equipment that doesn't leave the practice] [On computer equipment allocated personally to team members that they can take out of the practice] [On encrypted backup tapes or drives kept in a safe] [On cloud based software with digital storage] [As encrypted backups with digital cloud storage] [On cloud-based file hosting service such as One Drive, iCloud and Dropbox] Other:
How we store digital data within the EU	See (M 217C) for details of companies and agreements
How we store digital data outside of the EU, in the USA	See (M 217C) for details of companies and agreements

Information Flows

Please adapt the information flow tables to indicate your arrangements

Outgoing information flow		
Format	**Who to**	**How is it secured**
Email	Secondary care Referral practitioners Dental labs Patients Other:	Encrypted email [such as ShareFile] NHS Mail Other:
Fax	Secondary care Referral practitioners Dental labs Patient Other:	Sent to secure fax location only Other:
Post/ Courier – hard-copy or electronic media	Secondary care Referral practitioners Dental labs Patients Other:	Recorded delivery Registered post Signed for Digital media is encrypted Other:

Text Message	Patients Labs Other:	From secure practice owned phone only with encrypted message such as iMessage or WhatsApp
Other		

Ryedale Dental Healthcare Clinic AND IMPLANT CENTRE LTD

Incoming information flow		
Format	**Who from**	**How is it secured**
Email	Secondary care Referral practitioners Dental labs Patients Other:	Encrypted email [such as ShareFile] Receipt of email received NHS Mail Other:
Fax	Secondary care Referral practitioners Dental labs Patient Other:	Sent to secure fax location only Other:
Post/ Courier – hard-copy or electronic media	Secondary care Referral practitioners Dental labs Patients Other:	Recorded delivery Registered post Signed for Digital media is encrypted Other:
Text Message	Patients Labs: Other:	To secure practice owned phone only with encrypted message such as iMessage or WhatsApp

Sensitive information risk assessment

	Question	**Check if yes** **Yes = risk**	**If yes how to reduce the risk to the minimum**	**Sig and date when risk reduction complete**
1	Are you unaware or unsure of the guidelines on how to send out patient-identifiable information (M 217C)?			
2	Do you ever send out more patient-identifiable information than you think is necessary for the purpose of the data transfer?			
3	Do you ever receive more patient-identifiable information than is necessary for the purpose of the data transfer?			
4	Do you use memory sticks to transport patient-identifiable information?			
5	Do you send patient-identifiable information outside the European Economic Area without a registered process in place?			

	Email			
6	Do you regularly send out or receive patient data through non-NHSmail accounts?			
7	Are email attachments containing patient-identifiable information sent without any form of encryption or password-protection?			

	Question	**Check if yes** **Yes = risk**	**If yes how to reduce the risk to minimum**	**Sig and date when done**
8	Do you routinely send patient-identifiable information to non-business email accounts e.g. Yahoo, AOL?		**Text is written like this and**	
9	When emailing within your organisation, is the patient name routinely in the subject of your email?			
	Fax			
10	Do you send all faxes with patient-identifiable information to areas that are NOT designated as safe havens?			
11	Do you receive faxes with patient-identifiable information in areas that are NOT designated as safe havens?			
12	Are faxes containing patient-identifiable information sent out BEFORE recipients are phoned to warn them that you will be faxing this information?			
13	Are faxes containing patient-identifiable information sent out without cover papers?			
	Post			
14	Do you ever post patient-identifiable information to an insecure area?			

15	Do you send external post containing patient-identifiable information in unsealed envelopes or through internal mail envelopes?			
16	Do you ever send or receive post containing patient-identifiable information that is NOT marked as “Private & Confidential”?			
17	Do you send out bulk data on digital media without using secure courier services?			
	Other			
18	Do you ever send patient-identifiable information by text message?			

Ryedale Dental Healthcare Clinic
AND IMPLANT CENTRE LTD

Privacy Impact Analysis - Outcomes

After reviewing the results of:

- The Business Impact Analysis (M 217N)
- The Information Security section of Information Governance Procedures (M 217C)
- This Information Map and Risk Assessment

Write here if it is agreed that we have found the best ways to reduce or eliminate the impact on the privacy of individuals that arise from our processing of personal data:

Write here if there are any additional measures that we will take to reduce the privacy impact arising from our processing of personal data:

Privacy Impact Assessment signed off by:

Linda Williams the Information Governance Lead.

Signature: Date:

If you have any actions arising you can create a ToDo in the iComply Application Calendar.

The next Privacy Impact Assessment is scheduled in iComply application. If you are not an iComply member, write your next review date below.

Next review date (for non-members of iComply):

Ryedale Dental
Healthcare Clinic
AND IMPLANT CENTRE LTD