
















## Privacy by Design

Steps the practice is taking to prepare for the GDPR 2018

## Preparing for the General Data Protection

	Key people within this Practice are:-	Position
	<b>Charles Crawford</b>	<b>Principal Dentist / Data Controller</b>
	<b>Emma Stanley</b>	<b>Data Protection Officer/ / Practice Manager/ Data Processor</b>
	<b>Julia Crawford</b>	<b>Administration Manager/ Data Processor</b>
	<b>Matthew Byrne</b>	<b>Data Processor</b>
	<b>Matthew Kitchen</b>	<b>Data Processor</b>
	<b>Liam Wilson</b>	<b>Data Processor</b>
	<b>Audrey Chew</b>	<b>Data Processor</b>
	<b>Anna Lewis</b>	<b>Data Processor</b>
	<b>Chui Yan Chu</b>	<b>Data Processor</b>
	<b>Joanne Davies</b>	<b>Data Processor</b>
	<b>Stacey Cowgill</b>	<b>Data Processor</b>
	<b>Fiona Horrocks</b>	<b>Data Processor</b>
	<b>Cathleen Lancelott- Redfern</b>	<b>Data Processor</b>

This template is an audit of all the data held within the practice of key assets. This document shows how you use and share any personal data to comply with GDPR. (The last 5 rows are not mandatory therefore)

Audit Review:- 15 <sup>th</sup> March 2018											
Name of asset	What does it contain	Location	Owner	Volume	Personal data	Who can access	Shared	Form	Retention	Impact	Key asset
Patient Records											
Patient Records (Paper)	Personal and medical history, Contact details, Treatment details	Secure by lock in: Filing cabinet Attic	Data Controller Charles Crawford Data Processor See list above	Estimate of patient records 5000	Yes; includes sensitive personal data	Access is restricted to Staff member <u>ONLY</u>	Information is shared with staff within the practice and with consent NHS and other referring dentist and other professional bodies e.g GDC	Paper folder	11 years or age 25 which ever longer.	Loss of Confidentiality: Patient safety impact; - privacy impact; Loss of Availability: Loss of Integrity:	Yes
Patient Records (Digital)	Personal and medical history, Contact details, Treatment details	Secured locally on a hard-drive server, and by hosted storage through the internet with Systems for Dentists	Data Controller Charles Crawford Data Processor See list above	Estimate of patient records 10000	Yes; includes sensitive personal data	Access is restricted to Staff member only with <u>password</u>	Information is shared with staff within the practice and with consent NHS and other referring dentist and other professional bodies e.g GDC	Digital	11 years or age 25 which ever longer.	Loss of Confidentiality: Patient safety impact; - privacy impact; Loss of Availability: Loss of Integrity:	Yes
Patient Radiographs (wet Film)	Radiograph image	In paper folders in attic	Data Controller Charles Crawford Data Processor See list above	Estimated proportion of total patients records 3000	Yes	Access is restricted to Staff member <u>ONLY</u>	Information is shared with staff within the practice and with consent NHS and other referring dentist and other professional bodies e.g GDC	paper	11 years or age 25 which ever longer.	Loss of Confidentiality: Patient safety impact; - privacy impact; Loss of Availability: Loss of Integrity:	Yes
Patient Radiographs (Digital)	Radiograph image	Secured locally on a hard-drive server, and by hosted storage through the internet by Digital Dental /Sopro	Data Controller Charles Crawford Data Processor See list above	Estimated proportion of total patients records (Since into of Digital system) 6000	Yes	Access is restricted to Staff member only with <u>password</u>	Information is shared with staff within the practice and with consent NHS and other referring dentist and other professional bodies e.g GDC	Digital	11 years or age 25 which ever longer.	Loss of Confidentiality: Patient safety impact; - privacy impact; Loss of Availability: Loss of Integrity:	Yes
Models	Scale reproduction of patients dentition	Secure by lock in: Attic	Data Controller Charles Crawford Data Processor See list above	Estimated proportion of total patients records 1500	Yes	Access is restricted to Staff member <u>ONLY</u>	Information is shared with staff within the practice and with consent NHS and other referring dentist and other professional bodies e.g Dental Labs	Gypsum	11 years or age 25 which ever longer.	Loss of Confidentiality: Patient safety impact; - privacy impact; Loss of Availability: Loss of Integrity:	Yes
Models Digital	3D Digital scanned image capable of reproduction	Secure by hosted storage through the internet with Planmeca	Data Controller Charles Crawford Data Processor See list above	Estimated proportion of total patients records (Since into of Digital system) 50	Yes	Access is restricted to Staff member only with <u>password</u>	Information is shared with staff within the practice and with consent NHS and other referring dentist and other professional bodies e.g Dental Labs	Digital	11 years or age 25 which ever longer.	Loss of Confidentiality: Patient safety impact; - privacy impact; Loss of Availability: Loss of Integrity:	Yes
Staff Records											

Employment Records Paper	Photo ID, E-DBS Disclosure Number Personal details Right to work in UK, Medical details/GP/Hep B Vacc Contract Disciplinary record etc.	Secure by lock in: Filing cabinet	Practice owner Charles Crawford Responsible person Emma Stanley	All Staff	Yes	Access is restricted to the nominated responsible person Emma Stanley	Information is shared with CQC Nominated Person or PM or that member of staff	Paper	It's recommended that personal information of employees, including contact details, appraisals and reviews be kept for at least 6 years. You should keep hold of employees' financial for at least 3 years as HMRC may request to see them in this time.	Loss of Confidentiality: privacy impact; Loss of Availability: Loss of Integrity:	YES
Employment Record Digital	Photo ID, E-DBS Disclosure Number Personal details Right to work in UK, Medical details/GP/Hep B Vacc Contract Disciplinary record etc.	Secure by Password protected Computer and Email	Practice owner Charles Crawford Responsible person Emma Stanley	All Staff	Yes	Access is restricted to the nominated responsible person Emma Stanley	Information is shared with CQC Nominated Person or PM or that member of staff	Digital	It's recommended that personal information of employees, including contact details, appraisals and reviews be kept for at least 6 years. You should keep hold of employees' financial for at least 3 years as HMRC may request to see them in this time.	Loss of Confidentiality: privacy impact; Loss of Availability: Loss of Integrity	Yes
Training	CPD Courses PDP	Secure employment file by lock in: Filing cabinet	The individual staff member	All staff	Yes	Access is restricted to Staff member only	Information is shared with CQC,GDC Nominated Person or PM or that member of staff	Paper	5+years	Loss of Integrity with regard to professional training	Yes
Registration & Indemnity	GDC	Secure employment file by lock in: Filing cabinet Cupboard	The individual GDC registrant	Insert number of GDC registrants 10	Yes	restricted to the individual registrant and the Nominated person (CQC)	Shared upon request with CQC,GDC,NHS	Paper	6 years	Loss of Confidentiality: privacy impact; Loss of Availability: Loss of Integrity	Yes
Practice Finance											
Patient payment plans	Personal finance details and records of payment	Secured locally on hard drive, and by hosted storage through the internet by SFD	Practice owner Charles Crawford Responsible person Julia Crawford	Enter the number of patients in the plan 200	Yes	Access is restricted to the nominated responsible person Julia Crawford Emma Stanley	Information is shared with the Patient plan Provider admin staff in practice and patient upon request.	Digital	Accounting records should usually be kept for at least 6 years from the end of the financial year or accounting period to which they relate.	Loss of Confidentiality: Loss of Availability: Loss of Integrity	Yes
Patient outstanding invoice(s)	Personal finance details	Secured by hard drive And on hosted storage through the internet by SFD	Practice provider Charles Crawford Responsible person Emma Stanley Admin staff Julia Crawford Stacey Cowgill Joanne Davies	Number of invoices outstanding	Yes	Access is restricted to the nominated responsible person Julia Crawford and Emma Stanley	Information is only shared with the patient	Digital	Until payment is made and receipt is given	Loss of Confidentiality: Loss of Integrity	Yes
Practice Financial DD/Invoice (credit Licence maybe required)	Personal finance details	Secured by hard drive and on hosted storage through the internet by SFD	Practice provider Charles Crawford Responsible person Charles Crawford	Number of patients spreading cost of treatments	Yes	Access is restricted to the nominated responsible	Information is only shared with the patient	Digital	Until full payment is made and receipt is given	Loss of Confidentiality: Loss of Availability: Loss of Integrity	Yes

			Admin staff Julia Crawford Emma Stanley And patient	over a number of months.		person Julia Crawford Emma Stanley and patient					
Staff Payroll	Staff finance details NI Pension Sickness payment Benefits etc	Secured with password protected laptop and encrypted document	Practice provider Charles Crawford Responsible person Julia Crawford Admin staff Emma Stanley And Staff member Payroll agency	Number of staff currently employed 8	Yes	Access is restricted to the Julia and Charles Crawford	Information is shared with the staff member	Paper and Digital	Accounting records should usually be kept for at least 6 years from the end of the financial year or accounting period to which they relate.	Loss of Confidentiality: Loss of Availability: Loss of Integrity	Yes
Practice Accounts	Practice finance details	Secured storage safe from (Fire, Flood or theft) Digital records on a secure updated laptop with encryption	Practice provider Charles Crawford Responsible person Julia Crawford	Annual accounts for at least 6 years +	No	Access is restricted to Charles Crawford and Julia Crawford	The accounts are controlled by the nominated provider of services. They may be prepared by accountants and shared on request by HMRC	Paper Digital	Accounting records should usually be kept for at least 6 years from the end of the financial year or accounting period to which they relate.	Loss of Confidentiality: Loss of Availability: Loss of Integrity	Yes
Practice Admin Record											
maintenance Contracts	Equipment/Ser vice and supply contracts	Secured by lock in: Filing cabinet	Practice provider Charles Crawford Responsible person Emma Stanley	Number of Equipment/Ser vice and supply contracts held 11	No	Access is restricted to the Emma Stanley	the information is shared with the service/supply contractors & CQC	Paper Digital	The length of the contract (Note waste consignment notes 3 years) records of compliance may have extended retention periods.	Loss of Availability: Loss of Integrity	No
Mandatory Registrations	ICO Data Registration Employers Liability	Displayed	Practice provider Charles Crawford	As required annual renewal	No	All	All	Paper	Company registers should be kept for the entire life of the company.	Loss of Integrity	Yes
CQC Registration	Practice details and regulated service provided	Digital files	Practice provider Charles Crawford Nominated Responsible person Emma Stanley	Current files relating to this location	No	Available online (public)	Available online (public)	Digital	Throughout the duration of the business and then archived by CQC	Loss of Integrity	Yes
Log books	Essential equipment record/validati on	Paper/Digital	Practice provider Charles Crawford Responsible person Emma Stanley	Log book for each piece of equipment X3 years	No	Access is restricted to the nominated Staff Responsible person Emma Stanley	the information is shared with the service/supply contractors & CQC and other staff members	Paper Digital	3 years	Loss of Integrity	Yes

### **Step 3:- Communicating privacy information**

When you collect personal data you need to explain what data you wish to hold and why it is needed. This can be done by means of a published Statement which invites patients to request more detailed information.

A new consent notice will be available on the electronic tablet for patients to sign, introducing in April 2018.

A new medical history form will be introduced in April 2018, informing patients of data retention and transportation to third parties if necessary on a need to know basis.

A publish statement given to existing patients at examinations and published on the practice website ( see appendix 1) introducing in April 2018.

Under the GDPR there are some additional things you will need to tell people.

- ✓ Your lawful basis for processing the data
- ✓ Your Data retention period
- ✓ That individuals have a right to complain to the ICO (Information Commissioners office) if they think there is a problem with the way their data is handled.

### **Step 4:- Individuals' Rights**

Data subjects (people whose personal data is being held by your Practice) have certain rights:

- Right to be informed
- Right of access: see step 5 below subject access
- Right to rectification i.e. the right to require the rectification of any inaccuracies of personal data.
- Right to erasure i.e. the data subject has the right to require the erasure of personal data concerning them. However, this is qualified by the lawful basis as a healthcare provider to retain personal data in connection with the patients care and treatment. (subject to Step 6 below which would not permit erasure of treatment records)
- Right to restriction of processing i.e. subject to certain exemptions a data subject has the right to restrict processing of their personal data. (e.g. where the information accuracy is contested, the processing is unlawful, or data is no longer required by the Data Controller)
- Right to data portability i.e. the data subject has the right to receive their personal data which is held by you in a structured, commonly used format.
- Right to object i.e. the data subject has the right to object on grounds relating to the processing of their personal data. (e.g. personal profiling carried out that is not in connection with the public interest).

All the above information to be published onto the practices website and to train reception staff to signpost patients requiring this information. To be introduced in April 2018.

### **Step 5:- Subject Access Request**

GDPR grants people whose personal data is being held (known as Data subjects) by your Practice the right to access such personal data. This is referred to as a subject access request. Such requests by data subjects for the information held about them must be responded to promptly (within a month).

Practices need to update how they manage requests for information. In most cases, practices may not make a charge for providing this unless it can be shown that there is a material cost e.g. copying of radiographs. A practice may refuse or charge if a request is considered manifestly unfounded or excessive. If you refuse a request, you must explain without delay that the patient has a right to complain to the supervisory authority such as the ICO.

A new policy in the request of personal data to be introduced by June 2018. To include all the above information.

### **Step 6:- Lawful basis for processing personal data**

You should identify why you need to keep and process information. You may wish to publish a short Statement which invites patients to request more details. (Peoples Rights under GDPR).

We also need to keep accurate personal data for all staff who work with us in order to fulfil our obligations as employers and as providers of care in the healthcare sector.

To add to the new policy as above. Example below

All staff to have up to date personal information at the practice, to include GDC certification, DBS checks, immunisations, Hep B clearance and any boosters, Indemnity and CPD to be fully updated by August 2018.

## **STATEMENT of Calm Dental Care**

### **We will keep your records safely**

This practice complies with the Data Protection Act (1998) and General Data Protection Regulation (GDPR) 2018. This means that we will ensure that your information is processed fairly and lawfully.

We need to keep accurate personal data about patients in order to provide you with safe and appropriate dental care. We also need to process personal data about you if we are providing care under NHS arrangements and to ensure the proper management and administration of the NHS.

We invite you to request full details about how we do this from Reception

### **Step 7:- Consent**

Our patients provide us with personal data upon registering with you as a patient of the practice. This includes

- Name
- Address
- DOB
- Preferred means of contact
- Full medical history
- Patient records that we keep of treatment received.
- X-ray pictures & Models

We need to reassure patients that we will keep this information secure all the time they remain a patient of the practice (and for 11 years or age 25 after they were last seen) and that we will not share such information with any third party without their consent (such as for a referral to another practice, hospital or to payment plan provider). Please see Step 4.

Since this information is essential for the safe care and treatment of patients within the Practice, it is not necessary to obtain consent to hold this data. It is however necessary for us to establish how you would manage or transfer the data or how the patient wishes to be contacted.

We are not required to automatically “repaper” or refresh all existing Data Protection consents in preparation for GDPR. But if you rely on individuals’ consent to process their data, make sure it will meet the GDPR standard on being specific, clear, prominent, opt-in, properly documented and easily withdrawn.

Please be aware if you use in anyway Gmail or similar services that say they share their data with other parts of their organisations and 'trusted' (read paid for) 3rd parties, this is another area of potentially sharing data that you are responsible for. This should include a consideration of how you use the internet to communicate with patients.

RP4 suggest a simple additional questionnaire to be completed by all existing patients perhaps when they are reattending for an examination appointment and when you are updating and signing a Medical History. This is to confirm the data that you hold for them is correct and to confirm their preferred method of contact by the Practice (telephone/email/text). See **Appendix 2**

We will also hold and process personal data of staff members and people applying to work within your Practice. All such data must be held securely and not be accessible by other unauthorised staff members. Remember that some personal data may be accessible to the practice accountants and staff must be aware that this information will be processed by an authorized third person therefore. Clearly it is necessary to retain such data as may be requested for examination by the CQC or HMRC in an investigation.

The ICO however makes the point that no such data should be held beyond a time when it might reasonably be required. HMRC require that accounting information that may include staff payments be retained for 7 years. No data should be kept because it ‘might be useful on a rainy day’.



Staff members upon leaving employment have a right to have their information removed, see Step 4. It should be remembered that this may affect the ability of the practice management to provide a detailed reference of employment however. Financial details will need to be retained for 7 years.

### **Step 8:- Children**

We treat children within the Practice and will need to obtain parental or guardian consent for any data processing activity ( e.g referral or contact for reminders etc) for children under the age of 13. Children's data should be treated in exactly the same way as that of an adult and of course children have the same rights as an adult (see step 4). Children merit special protection if or when we use their personal data for marketing purposes e.g. marketing ortho or gumshields.

### **Step 9:- Data breaches**

You should ensure you have the right procedures in place to detect, report and investigate a personal data breach.

As a dental practice we are already required to notify the ICO (and CQC and possibly other bodies) if we suffer a personal data breach. Failure to report a breach could result in a fine as well as a fine for the breach itself.

**It is imperative that the practice regularly updates its Data Security Policy and reviews how data is protected using effective encryption which prevents copying and reuse of data from for example a lost memory stick device.**

Updated Data Security Policy and Review to be performed by June 2018

Reception staff to be trained and updated in the giving and receiving of personal data by April 2018.

### **Step 10:- Data Protection by Design and Data protection Impact Assessments**

We should familiarise yourself with the ICO Code of Practice on Privacy Impact Assessments and work out how and when to implement them in your practice.

An example would be where you have installed CCTV in or around your practice building.

To discuss risks and benefits of introducing a CCTV system at the practice.

To produce PIA's for the practice by May 2018

### **Step 11: - Data Protection Officers**

Appoint a named officer for Calm Dental Care is Emma Stanley, however due to minimal information this is not added into the job duties or their job role.

Emma Stanley to attend regular updates and training sessions for GDPR throughout the year

### **Step 12: International**

Any international third parties used by the practice needs to have their written data protection document if outside the EU. For example Invisalign.

Request data protection policies for any non EU companies we transfer data to and hold written and digital records at the practice. To be done by May 2018.

### **Step 13: Protecting our Computer Systems**

It is essential we have up to date safety softwares such as antivirues and firewalls. This is to protect us from hackers, viruses and spamming.

Systems for Dentist are responsible for the safety of our patient records. However the practice needs to protect all computers from data breaches as part of the GDPR 2018.

New protection softwares to be installed on all computers with patient or employee information on. To be password protected and encrypted by June 2018.

### **Step 14: Social Media**

This is a policy for staff to adhere to the rules of the practice in regards to data breaches on social media. This can be found in the employee handbook.

New social media policy to be introduced and signed by all staff at the practice and kept in their personal file.

**The practice needs to purchase a new lockable and industrial filing cabinet in the office that holds employee information and patient account information. To be purchased by April 2018**

What the practice has done so far:

- Introduced a new, more personal reception desk. This has reduced patient access.
- A new system to keep lab work kept away from the public
- New Medical History forms made ready to be introduced
- An update scheduled to advise staff of our Privacy By Design
- New locks placed on the filing cabinets for added protection
- New burglar alarm systems put into place

This practice complies with the Data Protection Act (1998) and General Data Protection Regulation (GDPR) 2018. This means that we will ensure that your information is processed fairly and lawfully.

#### **What personal information do we need to hold?**

- Your past and current medical and dental condition; personal details such as your age, address, telephone number and your general medical practitioner
- We may need to request details of your NHS number and entitlement to healthcare treatment
- We may also need to request details of your exemption status
- Radiographs, clinical photographs and study models
- Information about the treatment that we have provided or propose and its cost
- Notes of conversations or incidents that might occur for which a record needs to be kept
- Records of consent to treatment
- Any correspondence relating to you with other health care professionals, for example in the hospital or community services.

#### **Why do we hold this information?**

We need to keep accurate personal data about patients in order to provide you with safe and appropriate dental care. We also need to process personal data about you if we are providing care under NHS arrangements and to ensure the proper management and administration of the NHS.

#### **Retaining information**

We are required to retain your dental records, X- rays and study models while you are a patient of this practice and after you cease to be a patient, for at least eleven years or until age 25, whichever is the longer.

#### **Security**

Your information is held in the practice's computer system and in a secure manual filing system.

The information is only accessible to authorised personnel. Personal information will not be removed from this practice without the patients authorised consent.

Your personal information is carefully protected by the staff at this practice. All access to information is held securely and can only be accessed by regularly changed passwords. Data is encrypted and computer terminals are closed if unattended.

#### **We may need to disclose your information**

In order to provide proper and safe dental care to:

- Your general medical practitioner
- The hospital or community dental services
- Other health professionals caring for you
- NHS payment authorities
- The Inland Revenue
- The Benefits Agency, where you are claiming exemption or remission from NHS charges
- Private dental schemes of which you are a member.
- Dental Laboratories

Disclosure will take place on a 'need-to-know' basis, so that only those individuals/organisations who need to know in order to provide care to you and for the proper administration of Government

(whose personnel are covered by strict confidentiality rules) will be given the information. Only information that the recipient needs to know will be disclosed.

In very limited circumstances or when required by law or a court order, personal data may have to be disclosed to a third party not connected with your health care. In all other situations, disclosure that is not covered by this Code of Practice will only occur when we have your specific consent. Where possible you will be informed of these requests for disclosure.

### PATIENT PREFERRED CONTACT METHOD

I confirm that my contact details are correct and I would prefer to be contacted by this Dental Practice by the following method (please insert preferred method and details)

Home or mobile telephone number:

Email address:

Text/SMS message:

Letter Post:

Address:

If I am unable to speak/receive a message/read any correspondence I authorise the Practice to Leave a message on this telephone number:

**OR**

Communicate with my Husband/Wife/Parent/Partner/Carer

Give Name:

Relationship:

Signed

Date

### Permitted use of personal data (STRIKE OUT CLAUSE A or B)

- A) EITHER, In the event that any person working at Calm Dental PRACTICE wishes to use any of my personal data for use for marketing, promotional, educational, training or any other purpose than my care and treatment; I permit the practice management to make an information request to me using the following method: Specify how to be contacted here:
- B) I do not permit the practice management to request using my personal data for any purpose other than my care and treatment.

NAME:

SIGNED

Date