The ROYAL COLLEGE of OPHTHALMOLOGISTS

# Confidentiality and Data Protection Policy

May 2018

# Contents

## *Document Control*

| | |
|---|---|
| Version/Date | 0.2, May 2018 |
| Status | For approval |
| Document Owner | Kathy Evans |
| Originator | Mike Andersson |
| History | 0.2 Annexes B and C updated<br>0.1 Initial Version |
| | |
| Version/Date | 0.2 August 2016 |
| Status | For approval |
| Document Owner | Kathy Evans |
| | |
| History | |

# 1 Introduction

To fulfil the College's role certain confidential information about individuals, including members and staff, as well as other matters is essential. It is imperative that, as a minimum, the College meets its legal and other obligations with respect to confidential information and this document sets out the Confidentiality and Data Protection Policy. As well as meeting minimum requirements, the College is committed to following appropriate best practice where applicable.

This policy is a key part of the College's overall approach to IG (Information Governance) and is primarily a reference document for management purposes. *Keeping Information Confidential and Systems Secure - A Guide for Staff* is a complementary document which sets out day-to-day and operational requirements. There is a separate policy for Information Security which covers ICT systems and their use as well as technical measures.

This policy and related documents have been developed taking into account key stakeholders including (current and past) College members at all levels, its staff and trustees, trainees, exam candidates and course attendees, as well as academic, scientific, commercial and other partners together with members of the public particularly those who are, or care for, patients with eye conditions.

The policy has been updated to reflect the provisions of the General Data Protection Regulation (GDPR) which takes effect from 25 May 2018.

# 2 Purpose and Scope

## 2.1 Information and Personal Data

This policy applies to information in all forms including text, numerical data, images or photographs, sound recordings and videos. Information may be held or stored in many different ways for example on paper or electronically in computers, smartphones, cameras or removable media such as memory sticks and cards, CDs or DVDs, and so on. It can be exchanged in many ways including by email, SMS (text message), telephone, fax, and in conversation or meetings.

As explained in greater detail later, "personal data" is a term used in the data protection legislation for any information about a living individual who can be identified from the data itself or from other information that is either already available or likely to become so. Names, addresses, postcodes, dates of birth, NI (national insurance) and NHS numbers, email addresses, photographs, images from CCTV and so on allow identification either on their own or in combination.

Confidential information is not confined to personal data (which is the only remit of the Data Protection Act). For example, commercial contracts are usually confidential as are exam papers (at least until the exams have been taken).

## 2.2 Staff

For the purpose of this document and related policies, staff refers not only to permanent employees but also temporary or agency workers and contractors, committee and group members, volunteers and so on who can have access to: confidential information held by the College, its IT systems or both.

## 2.3 Applicability

This document and related IG policies apply to:

- all information used by the College
- all information systems run by the College or on its behalf
- all staff.

Many requirements will apply to suppliers and other third parties. In each case the relevant requirements will be documented and enforced contractually and/or through data sharing agreements (DSAs).

# 3 Background and Requirements

## 3.1 Data Protection Act

The principal source of statutory requirement since 1998 has been the Data Protection Act (DPA) which implements the EU Data Protection Directive and applies to living individuals. From May 2018 the EU General Data Protection Regulation (GDPR) comes into force and it has been consolidated into a new Data Protection Bill which is currently going through Parliament and is likely to become the Data Protection Act 2018. Further information is provided in Annex A but, to set the context, the 6 "principles" of GDPR can be summarised as - Personal data must be:

- Processed lawfully, fairly and transparently.
- Collected only for specific legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Must be accurate and kept up to date.
- Stored only as long as is necessary.
- Ensure appropriate security, integrity and confidentiality

The act applies not only to computerised or digital information but also to paper-based filing systems.

## 3.2 Common Law Duty of Confidence

A duty of confidence arises when one person discloses information to another (for example patient to clinician or member of staff to employer) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation derived from case law and included in professional codes of conduct. When an individual has died, information relating to that individual remains confidential under the common law.

## 3.3 Patient Data

### 3.3.1 NHS Patients

For a number of reasons the College has access to and/or is data controller for certain NHS patient data. The NHS imposes a number of requirements on organisations in such a position and further information is given in Annex C.

### 3.3.2 Professional Codes of Conduct

All doctors are required to be familiar with and to follow the General Medical Council (GMC) publication *Good medical practice*. This has a detailed section on Confidentiality[1].

## 3.4 Other

### 3.4.1 Privacy and Electronic Communications Regulations

The Privacy and Electronic Communications Regulations (PECR) complement the General Data Protection Regulation and implement the European *e-privacy Directive* as it is known. Many of the regulations apply to providers of communications and networking services and therefore do not affect organisations like the College. However, the regulations do restrict "unsolicited marketing by phone, fax, email, text, or other electronic message". The regulations are also the source of the requirements, imposed in 2011, relating to "cookies" from websites. Essentially users have to be

[1] http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp

informed when cookies are used and what they are for before they can be stored. Cookies can only be stored with users' consent. Further information is available from a section[2] of the ICO web site.

### 3.4.2 Freedom of Information Act

The Freedom of Information Act (FoIA) applies only to public bodies and therefore the College is excluded. However, it should be noted that NHS organisations as well as other public bodies can hold information provided to them by the College and such information could be disclosed in a response to an FoIA request.

### 3.4.3 Financial Data

The PCI DSS (Payment Card Industry Data Security Standard) applies to cardholder data. Further information can be found at the PCI web site[3].

## 3.5 Duration of Obligations

Confidentiality obligations remain in perpetuity in the vast majority of cases.

## 3.6 Enforcement

The ICO (information Commissioner's Office) is responsible for enforcement of the General Data Protection Regulation as well as the Privacy and Electronic Communications Regulations.

Certain breaches of the General Data Protection Regulation are criminal offences for which both individuals and organisations can be prosecuted. However, the most common action taken by the ICO for breaches is to issue "Enforcement Notices" which require organisations to take specified actions to ensure they comply with the law. For serious breaches of the General Data Protection Regulation and the Privacy and Electronic Communications Regulations the ICO can serve "monetary penalty notices" of up to a maximum of £17 million or 4% of turnover

# 4 Roles and Responsibilities

## 4.1 All Staff

All staff (as defined above) are under legal and contractual obligations to keep personal and other information confidential not only during their employment (or equivalent) but also after it has been

[2] https://ico.org.uk/for-organisations/guide-to-pecr/
[3] https://www.pcisecuritystandards.org/

terminated. All information including notes and other papers which relate to the College's activities must be handed in upon termination of employment. No copies can be retained.

## 4.2 Chief Executive

The Chief Executive has overall accountability and responsibility for confidentiality and data protection. Operational responsibility is delegated to the data protection lead and the Chief Executive is responsible for ensuring that the role is performed. The data protection lead role may be shared between staff or combined with other roles but the responsibilities of the individual or individuals undertaking it must be formally documented when appointments are made. The data protection lead must be adequately trained in order to perform the role.

## 4.3 Data Protection Lead

The key responsibilities (in no particular order) of the data protection lead are to:

- regularly review, update as necessary and annually renew the College's DPA registration
- provide a point of contact for staff who need information, advice or support in connection with confidentiality and data protection matters
- ensure that this policy is reviewed regularly and kept up-to-date
- maintain the retention schedule for all information held by the College
- maintain relevant parts of the information asset register (IAR) - see below
- maintain privacy notices (formerly known as "fair processing notices")
- document procedures for regularly reviewing audit trails
- undertake reviews of audit trails to ensure there has been no inappropriate access to confidential information
- coordinate with and support staff with other IG responsibilities.

# 5 Risk Management and Assurance

## 5.1 Existing Information and Processes

All existing confidential information and its processing is summarised in the Information Asset Register (IAR). Each database or application processing personal data is fully documented as are flows of personal data.

## 5.2 New or Changed Information Sources and Processes

A structured approach, commensurate with the scale of change being proposed, must be taken whenever:

- any new data is to be collected
- acquisition, creation or implementation of any new application or database takes place
- any change to an existing application, database or operational procedure involving data takes place.

This is to ensure:

- options are appraised
- risks are managed
- operational continuity and data quality are maintained
- IG requirements including those for confidentiality and data protection continue to be met.

The ICO advocates "privacy by design" which it states[4] "is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether." An integral part of this approach are "privacy impact assessments" for which there is an ICO code of practice[5].

# 6 Procedures and Controls

This section outlines particular processes and controls the College has adopted or needs to highlight. However, data protection is an extremely broad subject and it is College policy to follow the guidance in ICO Codes of Practice[6] where applicable. Additional requirements for NHS data are covered in Annex C.

## 6.1 Data Collection and Uses

Where data is collected or entered manually care must be taken to ensure its quality in terms of accuracy, completeness, validity and consistency. When data is received electronically from other sources, its quality must also be checked as far as possible.

Existing data must be reviewed periodically to ensure it is still required, accurate and up-to-date. Data must not be processed simply because it is possible for some purpose if it was not specifically collected for that purpose in the first place.

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/
[5] PDF file: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
[6] A full list of ICO guidance documents can be found at: https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/

## 6.2 Access, Attribution and Audit

Access to data is restricted. It can only be accessed for defined purposes and by staff whose role requires them to do so.

All access to confidential data in IT systems is attributable to an individual and details of actions taken are stored in audit trails (which are protected against tampering). Audit trails are subject to regular review.

## 6.3 Data Storage

### 6.3.1 IT Systems

Confidential data that is not handled by an application must be stored in the appropriate designated folder on the main file server.

### 6.3.2 Paper

The College has a clear desk policy. In addition, confidential information must not be left visible when it is being worked on. All confidential information must be stored securely in lockable filing cabinets or as otherwise directed.

## 6.4 Data Transfer

### 6.4.1 Routine Procedures

Information is routinely exchanged and transferred by many staff as part of their day-to-day duties. *Keeping Information Confidential and Systems Secure - A Guide for Staff* covers use of email, file transfer, fax, SMS (text messages), phone calls and voicemail in such circumstances.

### 6.4.2 Portable Media

Use of portable media (such as memory sticks and cards, external hard drives, CDs and DVDs and so on) for any regular/routine transfer of confidential information is against College policy. Any other use of such media must be approved in advance and in writing by the IT Director who will specify appropriate security measures such as the nature of encryption required. Any such approval must only be given after all other options have been considered and a risk assessment has been undertaken.

### 6.4.3 External Processing

Any processing undertaken by suppliers or other third parties must be in accordance with the relevant requirements of this policy. In each case the relevant requirements are documented and enforced contractually and/or through data sharing agreements (DSAs). Contracts and DSAs cover breaches and, in particular, reporting of any incidents as well as penalties.

Particular care must be taken with web and "cloud-based" services as suppliers may provide or use services which are based outside the UK or which result in personal data being transferred overseas. This can often be inadvertent - the technical nature of cloud-based services is such that storage and processing can take place almost anywhere - and data is typically replicated in several parts of the world to maintain availability as near to 100% as possible and to ensure it is backed up.

### 6.4.4 Overseas Transfers

If any overseas transfers of personal data are to be outside the EEA (European Economic Area), relevant ICO Guidance[7] must be followed. However, at present it is College policy not to share data outside the EEA and its DPA registration reflects this.

Transfer of NHS patient data outside the UK is subject to much stricter additional requirements as explained in Annex C.

## 6.5 Images and Audio

### 6.5.1 Photographs and Recordings

It is increasingly common to record and/or photograph presenters as well as participants at conference sessions, seminars, courses and meetings. Care must be taken when photographing individuals or recording them (in either audio or video format) in these cases or any other situations. The intended use of the resultant personal data must be explained or notified in advance so that individuals can object or opt out.

### 6.5.2 CCTV

CCTV must be operated in accordance with the relevant guidance in the ICO's CCTV Code of Practice[8]. Appendix 2 "includes a simple checklist for users of very limited CCTV systems where the full provisions of the code would be too detailed".

[7] https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/#international

[8] Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/
PDF file https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

## 6.6 Retention

Confidential personal information must not be kept longer than required for the original purpose it was collected for or received. There are, however, minimum retention periods for certain types of personal information such as for income tax and the DPA does not override any statutory requirements to retain records.

A retention schedule is maintained by the data protection lead to ensure the requirements for all information - confidential (personal or corporate) or otherwise - held by the College are documented.

## 6.7 Disposal

When disposal of any confidential information takes places, it must be undertaken securely and in particular:

- Paper documents must be shredded and confidential waste bins for this purpose are available in office areas. Contractors who dispose of confidential waste are required to provide certificates of destruction.
- Portable media issued by the College must be returned to the IT department for disposal. CDs and DVDs are destroyed by breakage. USB sticks, SD cards, external hard discs and similar storage devices are securely erased before disposal in accordance with the requirements of the *Information Security Policy*.
- ICT equipment of all types[9] must be securely disposed of in accordance with the requirements of the *Information Security Policy.*
- Any stand-alone photocopiers must be treated as ICT equipment as most models save documents to be copied in internal storage.

## 6.8 Breaches

Staff must report actual or suspected breaches of confidentiality or other incidents including near misses at the earliest opportunity as rapid reaction is often essential. All reported incidents will be logged, investigated and managed in accordance with the incident handling procedure set out in the *Information Security Policy*. All serious breaches must be reported to the ICO within 72 hours.

[9] This includes but is not limited to PCs, laptops, tablets, smart phones, fax machines, MFDs (multi-function devices), networking devices and telephone equipment as all digital equipment can hold confidential or other information such as passwords which must be kept secret.

## 6.9 Access Requests

### 6.9.1 Subject Access Requests

Through Subject Access Requests (SARs) the Data Protection Act, as amended by the GDPR, gives individuals the right to obtain information held about them. Such requests must be referred to the data protection lead who will acknowledge them on receipt and ensure a response is provided to valid requests within one month of receipt (subject to the exceptions for examinations as outlined below).

### 6.9.2 Examinations

Exceptions apply to subject access requests concerning examinations. Schedule 7 of the DPA extends the deadline for responses and exempts scripts.

### 6.9.3 Third Parties

There are certain circumstances where there can be a legal requirement to disclose confidential personal information without an individual's consent. For example, courts and tribunals have powers in this connection. Any such third party requests must be referred to the Chief Executive.

It is College policy not to disclose membership lists or members' contact details in response to unsolicited requests by outside bodies including conference organisers, other professional bodies or commercial organisations.

# 7 Related Policies and Guidance

Related College policies and guidance documents are:

- *Information Governance Strategy and Policy*
- *Information Security Policy*
- *Keeping Information Confidential and Systems Secure - A Guide for Staff*

ICO guidance on the Data Protection Act (and the Privacy and Electronic Communications Regulations) can be located through an index[10] on its website.

[10] https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/

# 8 Policy Management

## 8.1 Review and Revision

This Policy is subject to regular review (at intervals of no more than two years) and its next scheduled review date is recorded as part of that process. Any changes or updates are approved in accordance with the College's standard procedures.

## 8.2 Dissemination and Compliance

It is the responsibility of the data protection lead to ensure the requirements of this policy and any changes to it are disseminated appropriately.

To increase effectiveness of implementation and compliance:

- day-to-day and routine operational requirements are covered in *Keeping Information Confidential and Systems Secure - A Guide for Staff*
- all staff are suitably trained on appointment to a post as part of their induction and this is followed by regular refresher training.
- compliance is a requirement of staff and third party/supplier contracts.

## 8.3 Monitoring

Means of monitoring compliance will be developed by the IT Manager who will provide regular reports to the Chief Executive.

# Annex A:

The Information Commissioners' Office has produced a guide to the GDPR which explains the provisions of the GDPR to help organisations comply with its requirements. It describes the guide as a "a living document" and states that it is working to expand it in key areas. Therefore, readers wanting to know the current advice from the ICO are advised to refer to the ICO website.[11]

# Annex B: Information Processed by the College

## B.1 Data Protection Registration

The College is registered (number: Z4988048) as a data controller with the ICO.

## B.2 Purposes

To fulfil its role and obligations the main purposes for which the College processes information about individuals include the following:

- membership list maintenance
- member services
- fundraising
- education and training
- events and courses
- examinations
- professional development and revalidation (including logbooks and e-portfolios)
- employment of staff and matters relating to other personnel such as volunteers, lay members and trustees
- surveys
- College management and administration
- premises operation and security (using CCTV)
- compliance with legal and regulatory responsibilities, including equalities monitoring.

Information is also collected about visitors to the College website and this is explained in the Privacy & Cookie Policy[11].

[11] https://www.rcophth.ac.uk/privacy-policy/

## B.3 Member Information

Information held on members includes identification and contact data (including name, address, date of birth, telephone number/s and email address) together with qualifications, specialities and appointments held. Information is also held in connection with College committee membership and roles such as CPD coordinator, examiner, regional adviser, or tutor.

College policy is not to provide member information to commercial third parties except for specific contracted purposes such as mailing of College publications, in connection with educational events or other matters of professional benefit.

Members who wish to make some of their information searchable by other members or the public have the following options.

- In the members' area of the College website:
  - allow other members of the College to search by name, hospital, and special interests.
  - as above but email address is displayed in search results.
- In the public area of the College website allow searches (for NHS Consultants only) returning name, hospital and specialties.

# Annex C: NHS Data

## C.1 Patient Confidentiality

Patient confidentiality is a complex and rapidly evolving area. In addition to the Data Protection Act, the GDPR and the Common Law Duty of Confidence, NHS organisations in England have to meet a wide range of requirements set out in legislation, NHS codes of practice and elsewhere. Some of the key sources of requirements include the following.

- NHS Act 2006
- Health and Social Care Act 2012
- Health Records Act 1990
- The Confidentiality NHS Code of Practice[12]
- The NHS Care Record Guarantee for England[13]

[12] http://systems.digital.nhs.uk/infogov/codes/confcode.pdf
[13] http://systems.digital.nhs.uk/rasmartcards/strategy/nhscrg

- Information Governance Toolkit[14].

There are many sources of official guidance on confidentiality in the NHS including for example:

- A guide to confidentiality in health and social care[15]
- A guide to confidentiality in health and social care: references[16]
- A list of information governance resources and FAQs provided by NHS England[17].

## C.2 Caldicott Principles

The Caldicott Principles[18] (developed in 1997 and revised in 2013) state the overriding requirements concisely.

**Principle 1 – Justify the purpose(s) for using confidential information**
Every proposed use or transfer of personal confidential information within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

**Principle 2 – Don't use personal confidential information unless it is absolutely necessary**
Personal confidential information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

**Principle 3 – Use the minimum necessary personal confidential information**
Where use of personal confidential information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of personal confidential information is transferred or accessible as is necessary for a given function to be carried out.

**Principle 4 – Access to personal confidential information should be on a strict need-to-know basis**
Only those individuals who need access to personal confidential information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

[14] https://www.igt.hscic.gov.uk/
[15] http://digital.nhs.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf
[16] http://digital.nhs.uk/media/12823/Confidentiality-guide-References/pdf/confidentiality-guide-references.pdf
[17] https://www.england.nhs.uk/ourwork/tsd/ig/ig-resources/
[18] https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx?tk=426203846961004&cb=ec92186c-8fe3-41ac-ad89-94e94ee7a5ee

**Principle 5 – Everyone with access to personal confidential information should be aware of their responsibilities**
Action should be taken to ensure that those handling personal confidential information – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

**Principle 6 – Comply with the law**
Every use of personal confidential information must be lawful. Someone in each organisation handling personal confidential information should be responsible for ensuring that the organisation complies with legal requirements.

**Principle 7 – The duty to share information can be as important as the duty to protect patient confidentiality**
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

## C.3 Sharing for Non-care Purposes

A distinction is made between using personal confidential data (PCD) for care and non-care purposes. The latter is defined as[19] "the use of information for a purpose that does not directly contribute to the diagnosis, care and treatment of an individual, or to the audit/assurance of the care provided".

Sharing for non-care purposes needs "to be defined and limited, and additional requirements such as recorded informed consent or evidence of support under section 251 of the NHS Act 2006 may be required to enable lawful sharing".

Section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001) allows "the common law duty of confidentiality to be set aside in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable". Applications for approval to use Section 251 support are considered by the HRA Confidentiality Advisory Group[20].

## C.4 Third-Party Requirements

College policy is that an appropriate contract and/or data sharing agreement (DSA) must be in place with any third party processing NHS personal confidential data (PCD) on its behalf. The minimum requirements of such a contract and/or DSA follow below. To meet the requirements of this policy

[19] https://www.igt.hscic.gov.uk/GlossaryTerms.aspx?term=non-care%20purposes
[20] http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/

document, a privacy impact assessment should be undertaken before the College enters into any data sharing agreement.

### C.4.1 DSA Content

In accordance with section 8 of the ICO's Data sharing Code of Practice[21], a data sharing agreement "should, at least, document the following issues":

- the purpose, or purposes, of the sharing
- the potential recipients or types of recipient and the circumstances in which they will have access
- the data to be shared
- data quality – accuracy, relevance, usability etc.
- data security
- retention of shared data
- individuals' rights – procedures for dealing with access requests, queries and complaints
- review of effectiveness/termination of the sharing agreement
- sanctions for failure to comply with the agreement or breaches by individual staff.

Section 14 of the same document provides further details. In addition to these basic requirements College DSAs must:

- require compliance with applicable NHS standards
- require immediate notification to the College of actual or suspected data breaches
- require a certificate of destruction to confirm data has been deleted when the agreement ends
- restrict processing of the data to the UK
- prohibit any processing or access to the data other than as specified by the College
- prohibit sub-contracting without prior written agreement.

Detailed technical requirements (e.g. for encryption) are set out in the College's *Information Security Policy*.

### C.4.2 Third-Party Security

College policy is that third-parties must have either a satisfactory NHS IG Toolkit score or certification to ISO 27001:2013[22].

[21] Available from https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/
[22] http://www.iso.org/iso/iso27001