BMA

GPs as data controllers under the General Data Protection Regulation

The GDPR is an EU Regulation which is directly applicable in the UK. It should be read alongside the UK Data Protection Act 2018 (DPA 2018). The GDPR and the DPA 2018 replace the Data Protection Act 1998.

March 2018

British Medical Association
bma.org.uk

GPs as Data Controllers under the General Data Protection Regulation (GDPR)

Summary

The GDPR and Data Protection Act 2018 replace the Data Protection Act 1998 with an updated and strengthened data protection framework, however, the key principles of the original Act remain unchanged. The most relevant changes for GPs in their role as data controllers are highlighted in the box below. The remainder of the guidance explains GP data controllers' responsibilities under the GDPR, and sets out the main themes of the legislation and what needs to be done to ensure compliance. The principles in the guidance apply to doctors working in private practice or other NHS healthcare settings.

Definitions

- The GDPR applies to 'personal data'. This means data which relate to a living individual who can be identified from these data, or from these data and other information which is in the possession of, or is likely to come into the possession of, the data controller.[1] Personal data include, for example, name, NHS Number[2] or a computer IP address. 'Personal data' which reveal the health status of an individual are 'special category' data under the GDPR.[3]

- The term confidential health data is used throughout the guidance. This term is intended to encompass 'special category' health data under the GDPR **and** data which are subject to the common law duty of confidentiality.[4]

Key changes under GDPR

- Compliance must be actively demonstrated, for example it will be necessary to:
  - keep and maintain up-to-date records of the data flows from the practice and the legal basis for these flows; and
  - have data protection policies and procedures in place.
- More information is required in 'privacy notices' for patients.
- A legal requirement to report certain data breaches.
- Significantly increased financial penalties for breaches as well as non-compliance.[5]
- Practices will not be able to charge patients for access to medical records (save in exceptional circumstances).
- Designation of Data Protection Officers

1 The GDPR is not applicable to deceased individuals.
2 In Northern Ireland, the Health and Care Number is used (HCN); in Scotland it is the Community Health Index number (CHI).
3 In relation to medical records, the GDPR applies to computerised and paper records.
4 Information is subject to a duty of confidence when it has been shared in circumstances which generate an obligation of confidence, for example, the relationship between a doctor and patient.
5 There are two levels of fines dependent on the type of infringement and severity of breach. (1) Fines of up to 10,000, 000 euros or 2% of total worldwide turnover. (2) Fines of up to 20, 000, 000 euros or 4% of total worldwide turnover.

What is a data controller?

– Under the GDPR the data controller is the organisation (or, sometimes, a 'person'[6]) that 'determines the purposes and means of the processing of personal data'.[7] In other words, the data controller has overall control of the data and decides how, why, what, when, where and for how long data are to be processed.

– GP practices are data controllers for the data they hold about their patients. Although almost all practices will have data that are processed on their behalf by third parties, for example their IT system suppliers, it is the practice as data controller that has the responsibility for compliance under the Regulation.

– Under the GDPR, a data processor processes personal data 'on behalf of the controller', for example IT system suppliers are data processors. A processor can only act in response to an instruction from the data controller. Any change in the processing arrangements or significant decisions about the data can only be made by or with the agreement of the data controller.

– The data controller has a legal responsibility to control the way in which a data processor processes data on their behalf. A contract must exist between the data controller and data processor that sets out these responsibilities and should include a range of specific criteria, for example, assurances that the data processor has adequate security measures in place. This would be particularly important should a data breach occur.

– In groups of practices or other at scale settings individual GP data controllers may agree to act as 'joint data controllers' providing the arrangement is reflected within the contractual documents between the practices.[8]

– As data controllers, practices retain responsibilities for handling all requests for access to the data, for example, subject access requests made by patients or requests from third parties such as insurance companies and solicitors.[9] GP data controllers may delegate these activities but remain responsible for the final output.

– Practices retain responsibility for ensuring that access to confidential data in the practice is subject to appropriate controls so that it can be accessed only by staff who are providing direct care to an individual patient.[10] All practice staff who have access to medical records as part of their role in providing direct care must have confidentiality clauses in their employment contracts. This is an important element of data controllers' general obligation to ensure the appropriate security of the data they hold and protect data against unlawful access.

– Other healthcare professionals who are not employed by the practice, such as community nurses or physiotherapists, can legitimately access or enter information into patients' medical records for direct care purposes. Individuals who have been given an honorary contract to provide direct patient care can also access confidential data for this specific purpose.[11]

6 A 'person' is a legal entity and the term can encompass both individuals and organisations.
7 The term 'processing' is extremely broad and encompasses holding, collecting, recording, obtaining or disclosing data or carrying out any operations on the data. In short, it is difficult to think of any activity in relation to data handling which would not be deemed as 'processing' under the GDPR.
8 Legal advice should be sought on joint data controller contracts. Should a breach occur all joint data controllers, or just one individual data controller, could be held responsible depending on who was at fault and what responsibilities are set out in the agreement.
9 The BMA has separate guidance document titled *Access to health records*: https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records
10 The GMC defines 'direct care' as '…activities that directly contribute to the diagnosis, care and treatment of an individual. The direct care team is made up of those health and social care professionals who provide direct care to the patient, and others, such as administrative staff, who directly support direct care.' General Medical Council (2017) Confidentiality, p. 70. When a healthcare professional (or someone working to support the healthcare professional) is providing direct care they have a 'legitimate relationship' with the patient.
11 An honorary contract does not provide a lawful basis for accessing confidential medical records for purposes other than direct patient care. In some limited circumstances, it might be appropriate for an individual to hold an honorary contract if they are assisting the practice with some aspect of direct care to patients and therefore have a legitimate relationship with patients, for example medicines management case identification.

Consent and other lawful bases for processing

Provision of direct care

- Explicit consent under the GDPR is distinct from implied consent for sharing for direct care purposes under the common law duty of confidentiality. The GDPR creates a lawful basis for processing special category health data when it is for the provision of direct care that does not require explicit consent. GP data controllers must establish both a lawful basis for processing **and** a special category condition for processing.

  - The lawful basis for processing special category health data for direct care is that processing is:

    'necessary... in the exercise of official authority vested in the controller' (Article 6(1)(e)).[12]

    It is also possible for NHS GP practices to rely on 'processing is necessary for compliance with a legal obligation to which the controller is subject' (Article 6(1)(c).[13]

  - The special category condition for processing for direct care is that processing is:

    'necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services...' (Article 9(2)(h)).

  - In addition to a GDPR Article 9 condition for processing, it is also necessary to identify an additional condition in Schedule 1 of the DPA 2018. For the provision of direct care the relevant condition is *'Health or social care purposes'* (Schedule 1, Part 1 (2)).

- When relying on Articles 6(1)(e) and 9(2)(h) to share data for the provision of direct care, consent under GDPR is not needed. However, in addition to the GDPR, data controllers must also satisfy the common law duty of confidentiality. In order to satisfy the common law data controllers can continue to rely on implied consent to share confidential health data for the provision of direct care.[14] The most common example of when consent can be implied is when a patient agrees to a referral from one healthcare professional to another. In these circumstances, when the patient agrees to the referral this implies their consent for sharing relevant information to support the referral (unless the patient objects). The referral information can then be disclosed under GDPR using articles 6(1)(e) and 9(2)(h) as above.

Purposes other than direct care

- For purposes other than the provision of direct care and if a practice is relying on explicit consent as the legal basis for processing, the GDPR sets out certain requirements in order for consent to be valid: consent must be 'freely given, specific, informed and an unambiguous indication of the data subject's agreement'. If explicit consent does not meet these four criteria it will almost certainly be invalid for the purpose of the GDPR.[15] It is important to remember that explicit consent under the GDPR is distinct from common law reliance on implied consent for direct care as set out above.

12 This condition is applicable for GPs who carry out NHS work. The 'official authority' is NHS England's powers to commission health services under the NHS Act 2006 or to delegate such powers to CCGs. Private practitioners, as non-public authorities, will need to find an alternative lawful basis and could use Article 6 (1)(f) '... legitimate interests...'.

13 It is possible to rely on this condition because practices have contracts with NHS England to deliver primary care services.

14 This is in-line with GMC guidance. General Medical Council (2017) Confidentiality: good practice in handling patient information, paras 26 – 29. Implied consent also covers access for local clinical audit purposes, provided this is carried out by the direct care team.

15 It is important to note that the Article 29 Working Party guidance on consent takes a strict interpretation of the four criteria which underpin explicit consent: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849 (accessed 2 March 2018).

– Where there is a legal requirement to disclose, for example, a direction under the Health and Social Care Act 2012 or disclosures under public health legislation, the lawful basis for processing would be:

  '... for compliance with a legal obligation...' (Article 6(1)(c)).

  In the majority of cases, the most appropriate special category condition for processing in the face of a legal requirement to disclose will remain as:[16]

  '...for the purpose of preventative...medicine...the provision of health or social care or treatment or the management of health or social care systems and services...' (Article 9(2)(h)).

– When processing data for medical research the Article 6 lawful basis is 6(1)(e) '... for the performance of a task in the public interest...' The special category condition is Article 9(2)(j) '...research purposes...'. Reliance on this Article 6 lawful basis and Article 9 condition means that explicit consent is not required for GDPR purposes, however, explicit consent or another legal basis is still required under common law – see section below on 'dealing with requests for confidential health data'.

– In addition to a GDPR Article 9 condition for processing, it is also necessary to identify an additional condition in Schedule 1 of the DPA 18. For medical research the relevant condition is *'Research etc'* (Schedule 1 Part 1 (4)).

– Where there is a request for personal confidential data from an insurance company, solicitor, or employer (or similar third party) the lawful basis and lawful condition for processing will be explicit consent under both Articles 6(1)(a) and Article 9(1)(a).

Right to object

– Under the GDPR individuals have a general right to object to their data being processed in certain circumstances. This right applies unless the data controller can demonstrate 'compelling legitimate grounds for the processing'. [17] In the face of an objection from a patient, in many cases GPs are likely to be able to demonstrate 'compelling legitimate grounds' to continue holding the record because it is necessary for safe provision of direct care[18] and processing which is necessary for compliance with a legal obligation. Should a patient ask for their record not to be shared with another healthcare professional for the purposes of their own care then this should generally be respected.[19]

– Where the processing is for research purposes, the right to object applies unless it would prevent or seriously impair research which is carried out for reasons of public interest.[20] The onus is on the data controller to demonstrate that the 'public interest' in the research overrides an individual's expression of objection. This legal right to object is separate to any national opt-out model.[21]

16 Most legal requirements to disclose will be in relation to preventative health or the management of the health service.
17 Individuals also have the right not to be subject to a decision made solely by automated means – see p.7
18 Coupled with the associated medico-legal and contractual reasons to maintain accurate records.
19 Doctors should follow GMC guidance in this area. Where patients object to sharing for their direct care the potential consequences should be explained to them. General Medical Council (2017) *Confidentiality: good practice in handling patient information,* paras 30-31
20 The right to object can only be restricted when the 'appropriate safeguards' for processing special category data for research purposes are in place ie 'appropriate organisational and technical measures' (eg data security measures) and that the research will not cause distress to someone.
21 The legal right to object under the GDPR is different to the national opt-out model proposed by the National Data Guardian. This is a policy initiative which is intended to give patients certain choices about opting out of flows of confidential health data, including from NHS Digital – expected to be introduced in 2018. The national opt-out will also apply to approvals for use of data via regulations under s251 of the NHS Act 2006.

Data controller responsibilities for 'fair', 'lawful' and 'transparent' processing: privacy notices

- The first principle of the GDPR requires data controllers to process the data they hold 'fairly', 'lawfully' and 'transparently'.

- Fairness requires data controllers to be open and transparent about how data are used and that the data are handled in line with individuals' reasonable expectations. GP practices therefore must provide information in the form of 'privacy notices', sometimes referred to as 'fair processing notices', to their patients. These notices are a fundamental requirement of the GDPR and are required irrespective of the legal basis under which data sharing occurs.

- The GDPR requires that certain information must be included in privacy notices. For GP practices their practice privacy notice (PPN) must include:

  - Contact details of the practice as data controller;
  - Contact details for the data protection officer;[22]
  - The purposes for processing the data and the legal basis for processing the data – practices can state that processing is for direct patient care and quote Articles 6(1)(e) and 9(2)(h) as set out above;
    - other legal bases when processing for reasons other than direct care might, in England, include a direction under the Health and Social Care Act 2012 – PPNs should therefore also state that where disclosures are a legal requirement the lawful basis and special category condition for processing are: '…for compliance with a legal obligation…' (Article 6(1)(c)) and Article 9(2)(h) '…management of health or social care systems…';
    - for medical research the lawful basis and special category condition are Article 6(1)(e) '…for the performance of a task carried out in the public interest…' and Article 9(2)(j) '…research purposes…';

  - Information about with whom data are shared[23] – see below;
  - Any rights of objection which are available;
  - That patients have the right to access their medical record and to have inaccurate data corrected[24];
  - Retention periods – practices can state that GP records are retained until death;[25]
  - The right to lodge a complaint with the Information Commissioner's Office (ICO).

- This does not generally require every patient to be informed directly but the ICO expects reasonable attempts to be made to inform patients about how their medical records are handled.[26]

- The ICO suggests that a layered approach can be used. This means the provision of basic information available from a variety of different settings and in different formats with signposts to more detailed information, for example, the practice website or leaflet.

22 For most practices, the DPO is likely to be an employee of the Clinical Commissioning Group, Commissioning Support Unit, regional or local NHS Board, or Business Services Organisation which has responsibility for all practices in the area.
23 This includes details of any joint data controller arrangements (even though joint data controllers may not have access to personal data).
24 Where the practice and patient disagree about accuracy, a note should be added to the record to explain that the patient disagrees. The circumstances when information can be removed from medical records are extremely rare due to medico-legal reasons.
25 The NHS in all four nations publishes codes of practice for records management which include the standard retention periods.
26 The ICO has summarised the information that should be included in a privacy notice: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/?q=privacy+notices

Basic Practice Privacy Notice

– Every GP practice must have at least one PPN addressing their data flows relating to direct patient care. This must be prominently displayed on the practice notice board and prominently visible and readily accessible on the practice website explaining that the practice holds medical records confidentially and shares them with appropriate staff who are involved in providing direct care for individual patients. A notice or leaflet could also be given to patients when they register at the practice (or periodically if changes are made).

– Other notices must also explain when medical records are used for purposes other than direct patient care. These PPNs must include the information from the list above and any other information which is appropriate. There are two broad categories to which all practices are subject and common examples include:

Disclosures which are required by law or clinical audit requirements (England only)

'In order to comply with its legal obligations this practice may send data to NHS Digital when directed by the Secretary of State for Health under the Health and Social Care Act 2012'; and

'This practice contributes to national clinical audits and will send the data which are required by NHS Digital when the law allows. This may include demographic data, such as date of birth, and information about your health which is recorded in coded form, for example, the clinical code for diabetes or high blood pressure.'

Disclosures for medical research or health management purposes

'This practice contributes to medical research and may send relevant information to medical research databases such as the Clinical Practice Research Datalink and QResearch or others – when the law allows.'

Other common medical research databases or systems to which practices might contribute include SAIL (Secure Anonymised Information Linkage System in Wales[27]) and SPIRE (Scottish Primary Care Information Resource in Scotland[28]).

– It is important that the PPNs are kept up to date and are clearly visible in the practice – not hidden under later notices. Some practices have electronic notice boards which are an excellent way to ensure that patients are informed about these important matters. In addition to the notice board some practices include information with repeat prescriptions. It is advisable to provide as many links or prompts to the PPN as are feasible.

– Failure to provide reasonable 'fair processing' information to patients is likely to be a failure to comply with the GDPR. This might result in ICO enforcement action if the ICO agreed with a patient who complained that they were unaware of how their data had been processed.

– In relation to requests for access to patient records, for GP data controllers, a key aspect of 'lawful' processing is compliance with common law obligations of confidentiality.[29] When considering requests for access to confidential health data without patient consent GPs must be confident that there is an alternative legal basis for the disclosure.

Ensuring ongoing transparency – keeping patients updated

– Practices must ensure they continue to provide updated information to patients about new data sharing arrangements – for example, if a practice decides to contribute to a research database or project it must provide this information to patients. As well as updating the PPNs practices should notify patients using established channels such as waiting room notices, electronic displays, side notes on prescriptions, information

27 The PPN should signpost further information about SAIL: https://saildatabank.com/
28 The PPN should signpost further information about SPIRE: www.spire.scot
29 The BMA has produced a toolkit on confidentiality which covers the main aspects of doctors' duty of confidentiality: http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records

provided to patients at registration or when they attend the practice. If it is not practical to contact individuals directly via other means (post etc.) but the practice has the ability to provide alerts to patients relatively easily then the ICO has suggested this would be a reasonable expectation to ensure patients are informed. For example, where practices hold email addresses or mobile phone numbers for patients then an email or text alert should be used to bring to their attention this new use of their data and invite them to read the updated PPN.

Accountability: demonstrating compliance

– The GDPR requires data controllers to be accountable and to actively demonstrate compliance. Some elements of compliance with the GDPR can be demonstrated via the Data Security and Protection Toolkit in England.[30] Three essential indicators for demonstrating compliance are set out below.

Documenting flows of data from the practice

– GP practices must be aware of, and understand what, data they process, including via third party data processors (for example, system suppliers). This will involve the practice maintaining, and keeping up to date, records or an 'information register' of the data flows in which the practice participates. These records must include:

  – name and contact details of the data controller;
  – what personal data are processed (categories of data are sufficient, eg health data);
  – who the data subjects are (ie patients);
  – the data which flows from the practice in identifiable form and the purposes for processing;[31]
  – with whom the data are shared and the legal basis for the flow of data (as above the legal bases will be Article 6(1)(c), Article 6(1)(e) and Article 9(2)(h) and, for medical research, Article 9(2)(j); the legal basis may also be explicit consent (Article 6(1)(a)) where appropriate, for example, when sharing with insurance companies or solicitors);
  – the data sharing agreements the practice has signed up to;
  – a general description of the security measures, for example, data are encrypted when they are transferred between NHS organisations.

– Should the practice be subject to an inspection by the ICO or be the subject of a complaint it is likely that the ICO will wish to see these records or the information register as an important first step in establishing compliance.[32]

Policies and procedures

– Practices must have internal data protection policies and procedures in place. This will include policies for handling subject access requests, managing data breaches, managing requests for information from third parties (for example, insurance companies), staff training, managing infrastructure failures and remote access to data for mobile working.

Data Protection Impact Assessments

– A Data Protection Impact Assessment (DPIA) is mandatory when new processing arrangements (for example, the use of new technology) might result in risks to data subjects (patients). The ICO's 'DPIA screening checklist' lists the factors which must be considered to determine the risks of a new project.[33] One of these factors is processing health data 'on a large scale'. For the most part, processing by a smaller GP practice will not be considered to be 'on a large scale'. The other factors on the ICO list are unlikely to be activities which are routinely undertaken by GP practices, however, practices should still check the list as part of their consideration as to whether a new activity or change of process requires a DPIA.

30 https://www.igt.hscic.gov.uk/
31 Data which are effectively anonymised in-line with the ICO code of practice on anonymisation are not subject to the GDPR.
32 Data security matters may also form part of the CQC's assessment framework in England.
33 The checklist can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

– An example where a DPIA is likely to be required is if a practice was considering moving all of its records on all of its patients from one server to another. When carrying out a DPIA the practice must include a description of the processing, an assessment of the proportionality of the processing in relation to the purpose, an assessment of the risks posed and how the risk will be mitigated."

Dealing with requests for confidential health data

– When considering sharing confidential health data or when handling requests from other organisations, it is critical that GPs are confident that there is a clear legal basis for the disclosure. If there is no apparent legal basis for the disclosure GPs should not share the data and should seek further advice.[34] When an organisation is providing direct care[35] **and** has a legitimate relationship with an individual, the legal basis for sharing relevant information will be both implied consent to satisfy the common law[36] and under the GDPR it will be for the 'exercise of official authority…' (Article 6(1)(e) coupled with 'the provision of health or social care or treatment or the management of health or social care systems…' (Article 9(2)(h)). (See section above on consent and other legal bases for processing).

– Only information relevant for the specific purpose should be shared.

– Under common law, implied consent cannot be relied upon for sharing confidential health data with any organisation not providing direct care and which does not have a legitimate relationship with a patient or a group of patients.

– Where there are proposals for use of confidential health data for purposes other than direct care[37], for example, risk stratification or provision of services to patient populations, implied consent cannot be relied upon and another legal basis to satisfy the common law will be necessary, for example, a statutory requirement to share data or approval under section 251 of the NHS Act 2006 (in England and Wales). The onus is on the requesting organisation to make it clear to the GP which legal basis is being relied upon and how it has been obtained.[38] The GP must be confident that the legal basis is valid.

– Even if the GP data controller is satisfied there is a legal basis for the disclosure, where a substantial disclosure of confidential health data is proposed, for example national data flows to NHS Digital or data flows involving all practices within a CCG area, practices will still need to comply with the fair processing obligations so that there is transparency for patients. Such decisions will need to be made on a case-by-case basis and it might be necessary for the practice to seek further advice from its Data Protection Officer (DPO), a Caldicott Guardian,[39] the ICO or an information governance specialist. In some cases, it might be advisable to inform patients directly via letter, text or email where appropriate. Where there is a proposal for bulk disclosures, such as under the Health and Social Care Act 2012, direct individual level compliance with fair processing might be provided at a national level and practices should be guided by national advice on this.

34 Advice can be sought from defence bodies, the BMA, Caldicott Guardian or Data Protection Officer.
35 In line with GMC guidance, the term 'direct care' also covers local clinical audit undertaken by the team which has provided care and which has a legitimate relationship with the patient.
36 For example, when a patient agrees to a referral from the GP practice to a hospital.
37 Often referred to as secondary uses of information or indirect patient care.
38 Explicit patient consent, approval under s251 of the NHS Act 2006 (England and Wales) or certain statutory requirements, for example, the Health and Social Care Act 2012 (in England) can provide a legal basis. In rare and exceptional circumstances, information can be disclosed when there is an overriding public interest in disclosure, in-line with GMC guidance on confidentiality.
39 A senior person responsible for protecting the confidentiality of patient information and providing advice to staff to enable appropriate information sharing.

Breach reporting and rights of data subjects to seek compensation

– Under the GDPR it is mandatory to report a breach to the ICO if it is likely to result in risks to people's 'rights and freedoms'. The threshold to determine whether a breach needs to be reported depends on the risks. The ICO has yet to produce definitive guidance on breach notification, however, it seems likely that most, if not all, breaches of the confidentiality of confidential health data will amount to a risk which would warrant reporting. A breach must be reported to the ICO no later than 72 hours after the data controller becomes aware of it.[40]

– Similarly, data processors must notify the data controller without undue delay after becoming aware of a data breach.

– It is important to note that patients (as data subjects) whose rights have been infringed under the GDPR can sue for compensation where they suffer damage or distress.[41]

Subject access requests

– Handling subject access requests is the subject of a separate BMA guidance document titled *Access to health records*.[42] In most cases, patients must be given access to their medical records free of charge, including when a patient authorises access by a third party such as a solicitor. A 'reasonable fee' can be charged if the request is manifestly unfounded or excessive, however, these circumstances are likely to be rare.

Additional concepts under GDPR

Data Protection Officers

– All practices which provide services under an NHS contract are public authorities[43] therefore it is mandatory that they designate, but not necessarily employ or retain, a DPO; a person with expert knowledge of data protection law. (A single-handed private practice which is not carrying out NHS work and does not carry out 'large scale' processing is unlikely to be required to designate a DPO).[44] Designation is a decision to be made by the practice. The DPO is expected to monitor compliance, however, responsibility for compliance remains with the data controller and data processor. Large practices and multi-practice groups are likely to have in-house DPOs but smaller practices may prefer to designate external DPOs that could for instance be provided by a Business Services Organisation or local/regional health board.

– The DPO must not carry out duties which result in a conflict of interests and must not hold a position that leads him or her to determine the purposes and the means of the processing of personal data – this requirement will vary depending on whether the DPO is an internal or external appointment. In most cases, the data controller will be the GP practice rather than an individual GP and that internal practice decisions about data processing (ie the purpose and means of processing) will be subject to the governance arrangements of the practice partnership. This means it might be possible for GP partners to fulfil the role of DPO provided the role is defined to avoid conflict of interests and decisions are documented.

40 Not all information needs to be provided at this point but the ICO will wish to know the potential scope of the breach and what plans are in place to mitigate it. Information on how to report a breach to the ICO can be found at: https://ico.org.uk/for-organisations/report-a-breach/
41 Practices must seek legal advice in such situations.
42 Available at: https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records This document is in the process of being updated.
43 Public authorities are defined in the Freedom of Information Act 2000. This definition is likely to be transferred across to the DPA 2018. The definition includes non-statutory organisations such as GP practices – both single handed practices and 'at scale' groups of practices.
44 Private practitioners are advised to seek legal advice on this issue.

Pseudonymisation

– The process of pseudonymisation replaces 'real life' identifiers, such as NHS Number[45] and date of birth, with unique codes or pseudonyms which do not reveal the original identity of the individual (unless access is given to the 'key' to reverse the pseudonymisation process).[46]

– Under the GDPR, personal data which have undergone pseudonymisation but 'which could be attributable' to an individual by the use of additional information should be considered to be identifiable information.[47] Personal data which have been pseudonymised may or may not identifiable depending on how difficult it is to attribute the code or pseudonym to a particular individual.[48]

– Pseudonymised data can be re-identified when access is given to the 'key' or code which unlocks the pseudonymisation process, therefore in order for data to be considered pseudonymous 'technical and organisational' measures must be taken to ensure that the 'key' is held separately from the pseudonymised data. Sometimes pseudonymisation processes can render data effectively anonymised, however, data controllers must ensure that the data are anonymised in line with the ICO code of practice on anonymisation before sharing.[49]

– Pseudonymisation services will be provided to GP practices in England by NHS England.

Right to erasure ('right to be forgotten')

– It is extremely difficult to envisage the circumstances when this right would apply to medical records. The right to erasure applies only in specific circumstances, for example, when the processing is no longer necessary or when the processing has been unlawful. It is extremely unlikely that these circumstances will be relevant in a health context.[50] This right is separate to requests for amendments to medical records. Whilst it will be extremely rare for information to be deleted from medical records, it is established practice that corrections or amendments can be made; however, the original information, along with an explanation as to why information has been corrected or amended, must remain as an audit trail.

Automated decision-making

– Patients have the right not to be subject to decisions made solely on the basis of automated decision-making processes (for example risk stratification or artificial intelligence) and which has a significant effect on them. The data controller is responsible for the automated decision-making tools, such as algorithmic decision support systems, which they deploy including the consequences of any such processing.[51]

Data protection by design

– This concept will generally lie beyond the scope of general practices which are reliant on national systems. In England, GP data controllers rely on a range of protections in these areas which are provided for them under the GP systems of choice (GPSoC) framework and practice/CCG agreements. In Wales, Scotland and Northern Ireland IT systems and protections are supplied by NHS Wales Informatics Services, NHS National Services Scotland and Business Services Organisation Northern Ireland respectively. Practices which deploy their own systems will be individually responsible for them. All practices should, however, remember that they have a general obligation to implement organisational and technical data protection measures in all processing activities.

45 HCN (Northern Ireland) or CHI (Scotland).
46 The GDPR defines pseudonymisation as: 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information'.
47 Recital 26 of the GDPR.
48 The policy position on pseudonymisation is under developed. The ICO is developing guidance in this area.
49 Information Commissioner's Office (2012) *Anonymisation: managing data protection risk, code of practice.*
50 The right to object also applies, however, a GP is highly unlikely not to have 'overriding legitimate grounds for the processing'. See section on 'right to object'.
51 The supplier of the automated decision-making tools is also likely to bear some liability in the event of a claim by a patient.

Data portability

– This concept will generally lie beyond the scope of general practices. The right applies only when the lawful basis for processing under the GDPR is explicit consent or the performance of a contract. As set out above, GP practices will be reliant on the 'legitimate interests' and 'provision of health or social care' bases for processing.

Important note

The information contained in this document is for general guidance only and cannot be relied upon as legal advice. The BMA accepts no liability for the accuracy of the information contained herein and you should always obtain specific legal advice separately before taking any action based on the information provided herein or if you are unsure as to how to act in any situation.

BMA
British Medical Association, BMA House,
Tavistock Square, London WC1H 9JP
bma.org.uk

© British Medical Association, 2018

BMA 20180150