Bedfordshire & Hertfordshire
Local Medical Committee Ltd

GDPR:

Understanding the impact on General Practice

Authors:

Dr Mary Hawking: retired GP from Dunstable; ex-EMIS user; committee member of the Primary Health Care section of the British Computer Society

Ian Herbert: health informatician for 39 years, initially as a GP system developer; then with the NHS and now as an independent consultant; committee member of the Primary Health Care section of the British Computer Society; Founding Fellow of the Faculty of Clinical Informatics; Fellow of the British Computer Society.

Dr John Lockley: former GP, now retired from clinical medicine but continues in medico-political, managerial and medical informatics roles; former Chair of the SystmOne National User Group and currently a member of its national committee; Founding Fellow of the Faculty of Clinical Informatics. Committee member of the Primary Health Care section of the British Computer Society.

Ms Cath Pearson: Practice manager, Flitwick; member of the BCCG IT steering group; member of national committee of the SystmOne National User Group.

We are health and/or IT professionals: none of us is a lawyer, though legal advice has been used while creating this document.

If, as a practice, you are simply looking for a list of things to do in order to comply with GDPR, then you could just go to Chapters 5 & 6 (though Chapter 6 isn't actually a complete list). However, we strongly suggest that instead you read this entire document, because in our estimation the key to dealing with GDPR and related issues such as consent is to *understand* the situation in a detailed, integrated and comprehensive manner.

The *latest* version of this document is constantly available to download, free, at
http://www.bedshertslmcs.org.uk/advice-and-guidance/gdpr/

Cover Image provided by PixaBay at www.pixabay.com

Contents

Cumulative list of significant changes

v8.2		Original version, published 11/4/2018
V8.5		Added 2 recommendations re limits of, and charging for, extracts from the record

1. Important caveats about this report

1. The General Data Protection Regulation (GDPR), published by the EU in March 2016, (https://gdpr-info.eu/) is due to be implemented throughout the EU (including the UK) by 25th May 2018. However, the UK implementation of the GDPR, the Data Protection Bill 2018, is not yet law in the UK.

2. As a result, there is:-
    a) No case law
    b) No list of legal precedents to refer to (though there are some parallel or antecedent legislation/examples to draw upon)
    c) No examples of the application or sizes of penalties to refer to
    d) No certainty about how national and supranational legislative and monitoring organisations will respond in practice (especially as certain current practices, though arguably illegal under current legislation, are pragmatically being permitted)
    e) No codes of practice
    f) No national implementation plan
    g) No specific implementation plan for UK health, or primary care
    h) No awareness of any derogations which may or may not be applied to the UK implementation of GDPR.

3. Although we have studied what has been written and said about the legislation itself, its UK implementation, and its possible consequences, there is still no complete certainty about the situation. Within our group we have some variation of opinions as to the possible impact of GDPR: this is to be expected given the complexity of the situation, and the absence of legislation, case law and guidance.

4. It is just possible that the UK legislation and its implementation may be amended as a result of the problems and concerns this document raises. We understand that at least some of the areas highlighted have already been notified to the appropriate authorities.

5. Consequently, this document can only represent our best efforts to understand the state of play regarding GDPR. Undoubtedly as further information becomes available some of these uncertainties will disappear. In addition, a great deal hangs on whether the legislation is initially implemented in a draconian or benign fashion. We hope it is the latter, because complex legislation like the GDPR needs time to bed in, for inconsistencies and paradoxes to surface, and for any previous practices which were possibly technically illegal to be resolved, derogated — or even pragmatically be allowed to remain for a time.

6. Although we have mentioned aspects of secondary care, this report is primarily aimed at primary care.

7. Finally, **if you become aware of any mistakes or information which is now out-of-date, please let us know** then we can amend this document appropriately. Email any comments to LMCadmin@bhlmc.co.uk and put *GDPRreport* in the title line.

2. Background

The EU's General Data Processing Regulation (the GDPR, aka EU Regulation 2016/679 https://gdpr-info.eu/) applies to the processing of data about *living people* that either identifies them, or enables their identification in conjunction with other data to which the data controller has access, or could have access. It replaces the previous EU personal data protection legislation, Directive 95/46/EC, which formed the basis of the UK Data Protection Act 1998 (DPA 1998) and similar national legislation throughout the EU. Like the original EU directive and the DPA 1998, it applies to personal data held in any form: digital, on paper, or in analogue form (pictures, sound recordings, etc).

Because it is a regulation rather than a directive, the GDPR is intended to be implemented 'as is' in each EU member state. However, each state can add derogations where the GDPR permits it if they so wish. The UK currently intends to leave the EU, but to support its intention to trade much as now with the EU after Brexit, it has opted to incorporate the GDPR into a replacement for the DPA 1998, the DPA 2018. The DPA 2018 is likely to include, or otherwise enable, derogations permitted under the GDPR to cater for other UK data-related legislation, notably the Data Directions in the Health and Social Care Act 2012 and any additional personal health data sharing that is enabled by Digital Economy Bill 2017 and its regulations.

The GDPR contains 173 Recitals describing its objectives and the reasoning behind its 99 regulations. It was published in March 2016 and is due to be implemented across the EU (which includes the UK until at least March 2019) on the 25th of May 2018. Although the UK is due to leave the EU in March 2019, EU regulations will require companies outside the EU to adopt equivalent standards after Brexit if they are to continue trading with the EU and process personal data about EU citizens.

In principle, these proposals are good. However, the devil is in the detail, and as the caveats in Section 1 of this document point out, authoritative and UK-specific detail is thin on the ground: the UK legislation to implement the GFDPR – the DPA 2018 – has not yet completed its journey through Parliament, nearly two years after the publication of the GDPR. Neither is it clear whether all existing GP systems can support the GDPR's requirements.[1] Taken together, these factors make a comprehensive trouble-free UK implementation of the GDPR by May 25th 2018 very unlikely.

Our concerns are widely shared by other interested and informed people in the medical Informatics world[2] (though we are also aware of many individuals and organisations saying that GDPR isn't/shouldn't be that much of a problem).

[1] At least one of us (WJL) also believes that there is a risk that the requirements of the GDPR will be so onerous, and the concerns about its large fines so great, that some practices will not want to run the risk of falling foul of GDPR and would therefore prefer not to share data at all, or at the very best, in a minimal form. Clearly, this would not be good for patient care.

2 The BMA has major concerns about both the DPA 2018 (URL impossible to obtain in the normal way: do a web search for "BMA" & "Data Protection Bill", which will then retrieve the BMA Parliamentary brief on the topic dated 11 December 2017) and the regulations attached to the Digital Economy Act 2017

3. What is the GDPR intended to achieve?

The objectives of the GDPR are summed up in Articles 3-11. Many of its proposals reflect existing law. Those below that are new or significantly changed from the DPA 1998 are indicated.

In short the GDPR provides for:

1. **More uniform data protection law across the EU**. However, the GDPR also explicitly permits national derogations to various elements of the GDPR, which will encourage the opposite.[3]
2. **The extension of the territorial coverage of EU data protection**, to cover European-based organisations processing personal data outside the EU, and non-EU based organisations outside the EU that use personal data about EU citizens for sales purposes, and/or collect behavioural information about EU citizens in the EU, e.g. for profiling.
3. The key issue with the GDPR, as with the DPA 1998, is '**are you obtaining and processing personal data lawfully**' — one ground for which is consent. A great deal of data sharing is likely to take place on a lawful basis other than 'consent'. The concept of 'legitimate interest**'** may be used to counter allegations of improper use.
4. **Where consent is the legal basis for data processing, it must be fully informed, explicit and recorded for each purpose**. Silence, pre-ticked boxes and implied consent will not constitute consent. This is new.
5. **A data controller must have a written agreement with any organisation – a data processor -- which processes its data on its behalf.**
6. **Where a data controller provides another organisation with a copy of some or all of the personal data that it holds, the recipient organisation becomes the data controller of the data it receives.** The GDPR is *not explicit* about recording the details of such sharing arrangements, but makes it clear (Article 14) that the data subjects have rights to the same kind of fair processing information from the recipient as they have from the original data controller. This suggests that any sharing arrangements should be documented and contain the same information – identity of the new controller and DPO; when shared; the kind of data to be used; purposes; etc.
7. **Stronger and more detailed data subject rights**, i.e**.** the 'power to access, power to erase, power to prevent, power to transfer their own data.' This includes the right for an individual to receive the data a data controller holds about them in text or a commonly used digital format, to get their data ported from one data controller to another[4] and (*except for healthcare data*) to be 'digitally forgotten'. Normally the data controller will not be able to charge a data subject for providing these services. The power to transfer one's data, have it erased, and the inability to charge, are new. **However, patients do *not* have the right to request that information in the record be removed, or altered simply because the patients they don't like the implications, or disagree with the clinician's opinion.**
8. **Stronger and more detailed obligations for data controllers and processors.** Besides supporting the data subject's new rights over their data, this includes the obligation to

[3] Any national variations must be as permitted in Article 6.2 and 3 (which gives nation-states considerable latitude).

[4] Whether this would cover a GP data controller sending patient data to the patient's solicitor or insurance company, as GPs do now for a fee, is not clear

record their standard data protection procedures and their application, which should be for all use cases. These are greatly extended.

9. **A strong emphasis on 'minimisation'**. This is sometimes referred to as 'proportionality' in the GDPR, and means 'sharing with the receiving party only the data necessary for (i.e. relevant to) the recipient's stated purpose(s)'. As is explained in various places within this document, but especially section 7, item 5, this causes significant issues for healthcare data processing.
10. **Use of non-identifiable data whenever it can satisfy the intended purpose(s)** which would then put the use outside the scope of the GDPR, as it does of the DPA 1998.
11. **Routine monitoring of the adherence to the GDPR by data controllers and processors**, who must document their data protection procedures and their application to their usage of personal data, including the legal basis for their use. Article 5 of the legislation says that 'the [data] controller shall be responsible for, *and be able to demonstrate*, compliance with the principles.' This is new.
12. **Organisations routinely controlling and/or processing significant amounts of sensitive personal data, such as health care providers, must have a Data Protection Officer (DPO)**. The DPO will ensure that Data Controllers and Data Processors have appropriate data protection procedures in place and that they adhere to them. This is new.
    Public authorities must always have a DPO when (if) they are processing large scale special category data pursuant to Article 9. GPs fall within the definition of public authorities.
13. **Much larger fines under the GDPR.** Under the DPA 1998, the maximum fine the ICO could levy was £500,000[5,6]. Under the GDPR it is dramatically bigger — a maximum of €20 million or 4% of annual global turnover, whichever is higher. Unlike the DPA 1998, fines may be levied for not having sound data protection processes in place and/or not adhering to them and/or not recording adherence to them, *not just data breaches*.

4. How will the GDPR impact on UK general practice?

1. GDPR Article (2)h explicitly permits the use of personal data *for the provision of health and social care*. Those treating patients no longer need to (and actually *cannot* under the GDPR) rely on implied consent to make their data processing lawful, as is currently the case. It does the same for those *providing preventive or occupational medicine, assessing the working capacity of employees or managing health and social care systems and services, or who have a contract with a health professional.* The people doing the processing must owe the patient/client a duty of confidentiality, see Article 9(3).

[5] In practice, the ICO has never issued a penalty higher than £400,000, even to a corporate body.

[6] Just under two years ago, a high-placed representative from the ICO said that no individual healthcare staff had been penalised (other than nominally), and gave the impression that they were very balanced and mature about it all. However, almost immediately the ICO fined a practice £250,000 for a single release of information, even though the breach was self-reported. On appeal the penalty was reduced to £40,000, an *enormous* amount of money for a handful of partners to bear: it could easily bankrupt a practice. The ICO felt that the failure wasn't just about the breach, but that the practice's policies were insufficient, and that the staff hadn't received adequate training — which the practice disputes.

2. Article 9(2)i permits the processing of health data *for public health purposes*. Among the accompanying — and rather weak — recommendations to safeguard the rights and interests of data subjects, it suggests that people doing the processing should owe the patient a duty of confidentiality.
3. Articles 9 (2)j and 89 permits the processing of health data *in the public interest, for scientific or historical research and statistical purposes* with generalised recommendations 'to safeguard the fundamental rights and the interests of the data subject.' While this type of processing is essential if healthcare providers and commissioners are to fulfil their functions, use under these articles:
    - should accord with patient expectations in general (recital 47), and
    - only occur where pseudonymised individual data or aggregate data will not suffice for the stated purpose(s), (recital 39).
4. The GDPR applies to all data about UK patients *and practice staff*, wherever it is processed by an EU-based organisation, including data stored in the Cloud. It also applies to UK patients when their data is processed by a non-EU-based organisation offering them goods or services or collecting behavioural data about them. This would presumably include any data exported during the use of software as a service.
5. Each practice, as Data Controller, must have a *written* contract with each organisation that processes their identifiable data on the practice's behalf, for example with EMIS, TPP, Vision, Microtest and DocMan, if they provide remote data storage and /or processing services for them. *This will also include contracts with firms who deal with the physical storage and/or processing of their data — e.g. shredding firms, firms disposing of old computer memory, etc.*
6. Each practice must have a Data Protection Officer (DPO), who is responsible for ensuring that that the practice's data processing activities, protocols, records and structures conform to the GDPR. *The DPO may be an external* ***organisation***, or a person, and may be shared by several practices. Because of the need for the DPO to be independent, the practice DPO cannot also make decisions about instances of processing of any personal data controlled by the practice. The DPO must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices. There is reference to certification of the DPO — which does not (yet) exist in the UK. They must also be properly funded, and report directly to the highest level of management within the organisation(s) they serve.
7. Practices must record any model data protection protocols that they create/use as well as individual data protection decisions, including which protocols and GDPR element(s) were the basis for making the decision, e.g. the legal basis for the processing concerned. In some cases this may be done for classes of processing activity: for example all sharing of *relevant* data for the provision of personal care, health service management and a few other purposes is explicitly permitted by Article 9 of the GDPR where the user owes the patient an obligation of confidentiality. The overall data protection record must be sufficiently comprehensive to demonstrate positively to the practice's DPO that the practice is, and has been, conformant with the requirements of the GDPR. The organisation needs to be able to demonstrate a regular audit of the types of data it holds, processes it uses and policies that it has in place.[7]
8. A data controller must subject a data processing operation that is likely to result in a high risk to the data subject's privacy to a formal **Data Protection Impact Assessment,** and the data controller must seek the advice of their DPO when doing so – qv Article 35(2). The controller

[7] The guidance on the ICO website is still being generated but the clear direction of travel for smaller organisations is to concentrate on planning at this stage so that detailed implementation will be properly informed.

must also consult the supervisory authority[8] if the Assessment indicates that there is indeed a high risk, qv Article 36(1).

9. As small businesses and partnerships, the vastly increased *maximum* fines for breaching the regulations, see 3.12 above, are causing great concern in general practices. We do not know how rigorous the enforcement of the regulations will be at the outset, or how large any fines imposed are likely to be for different types of offence. These fines cannot be insured against, as they are for criminal offences
10. The role of the 'Data Controller in Common' will still apply where it is now the case: there will therefore be joint liability. Those using TPP's SystmOne are already Data Controllers in Common.
11. Under existing legislation (which will continue under GDPR) any patient has the right (with certain exceptions, such as in relation to child safeguarding) to refuse access to specific data by certain (or indeed all) healthcare providers, *other than the one who created it*, which the data controllers must make as easy to do as sharing the record[9].
12. The GDPR explicitly states that its 'right to be forgotten' (i.e. for a data subject to have a data controller erase all or some of the data he or she holds about him or her) does **not** apply to healthcare data.

5. Specific impact on practices using TPP SystmOne

SystmOne is unique among UK primary health care systems in that it uses a single shared record (SSR). Written in the mid-90s, its concept of a centrally-held, single record sits awkwardly within the framework of the DPA 1998 which was never designed with the SSR concept in mind. Nevertheless, the ICO agreed its use, and its consent mechanism (EDSM) — which is being changed to conform to the ICO's more recent recommendations. *The independent SystmOne National User Group (SNUG)[10] which is firmly in favour of the SSR principle has for some years been pushing for changes to legislation which more closely take into account the specific (and generic) needs of the single shared record concept.*

The GDPR has also not been constructed with the single shared record in mind, leading to some uncertainties. A big problem here, however – not just with the GDPR but also with the DPA 1998 – is the complete absence of legal precedents to guide everyone in this new and advanced medical IT environment. Therefore, one of our recommendations is that there should be a formal examination of the ability of the GDPR to cope with the current and future needs of the generic 'single shared record'. The essence of the problem is that using a single shared record runs counter to the data minimisation principle which is embodied in both the DPA 1998 and the GDPR.[11,12]

---

[8] Presumably this would be the UK Information Commissioner (ICO).

[9] Whether all (any?) GP system suppliers *can* restrict the viewing of specific patient data to specific healthcare providers is uncertain.

[10] Two of the members of this report's authors (CP and WJL) are members of its national committee.

[11] However, **if** patients are made aware (beforehand) of the fact that their whole record is shared, **and** that they can declare material they consider particularly sensitive as private; **and** they have to give permission before their single shared record can be viewed, we cannot see a problem with the SSR under either the DPA 1998 or the GDPR, *because the patient has been informed and given his/her consent for her record to be used in this way.*

The consent mechanism under SystmOne is very powerful, but also complex to describe.[13] Essentially, it allows the patient *at each unit she visits* to decide two things:

- whether the information it creates about her can be put into the 'pool' of information about her that other organisations can see
- whether staff at that unit are allowed to see the contents of what is in her pool.[14]

Under SystmOne it is possible to mark an entry as 'not to be shared' (i.e. it doesn't go into the pool), but currently there is no mechanism to mark an entry as being viewable only by a specific organisation: it would have to be made private to the organisation which created that entry, or alternatively when visiting a particular unit, the patient should withhold consent entirely for that organisation to see any of her pooled information.

6. Duties of practices

Before the DPA 2018 comes into force, practices must, as things stand:

1. Conduct an audit of each collection of personal data that the practice holds. For each collection state the purpose(s) for which it is used by the practice, how and when it is collected (and updated, if indeed it is), the general kind(s) of data held about each person in it, the legal basis for its collection, when (if ever) it will be destroyed, who it is routinely shared with, for which purposes, the legal basis for the sharing, etc.
2. Conduct an audit of their data handling methods and policies. There is much advice, and templates, on the ICO website
3. Have a privacy policy, with agreed, *written* protocols in place & publicised *before* any data is shared/processed.
4. Create and publicly display a GDPR **privacy notice,** see the ICO guidance. These are the same as FPNs (Fair Processing Notices) and describe how data about the patient and staff data is routinely used (including what is routinely shared, and who with). For details of what GDPR FPNs should contain and the formats to use, see the ICO guidance.
5. Remove the use of implied consent entirely (though the use of the concept of 'legitimate interest' remains acceptable — see section 4 (7)).
6. Appoint a Data Protection Officer (DPO)[15] – who needs a certified understanding of the technical and legal aspects. **The level of knowledge, duties, level of accreditation, and**

---

[12] See the CCIO and CIO Networks discussion paper: *'Data sharing and data protection in healthcare'* (July 2017): it calls on national bodies to create regulations which better reflect the types of information sharing that are now both possible and desirable in healthcare.

[13] The description we give shows the effect of what happens, but doesn't actually describe the physical mechanism by which it is performed (i.e. the 'pool' is virtual, not physical.)

[14] Note that under EDSM it is physically not possible for an organisation to view the patient's detailed record without her permission, and following the ICO's recent recommendations and unlike the NHS Summary Care Record, there are no overrides to this mechanism (even for clinical emergencies).

[15] The DPO can be a person or an organisation. He/she/it is there to advise and 'ensure fair play', and is the contact for queries from a controller's data subjects and the supervisory authority (which, in the UK, is the ICO).

level of teaching of the DPO still have to be defined by the legislators, and there is no mechanism currently in place to train or certify DPOs.
DPOs must be appointed by public authorities when they are processing large scale special category data pursuant to Article 9. GPs fall within the definition of public authorities.

7. Create, or obtain, data processing procedures for all common data processing activities,
8. Create, or obtain, formats for recording instances of these activities.
9. The ICO has stated that completing the IG toolkit would provide a very strong basis of ensuring compliance with the GDPR going forward (see the webinar 'Data protection for small healthcare organisations' on the ICO website). (See section 8.6 below for a major implication of this.)

Before data is shared[16], practices **must**, as things stand:

10. Have contracts in place with *all* Data Processor(s) processing patient or staff data at the practices' behest.
    a. This implies as a minimum the standard GP system suppliers who almost universally hold practice data at their data centres[17,18]
    b. will also need to include organisations supplying add-on products such as DocMan
    c. plus *any firm handling the shredding and disposal of paper documentation or of redundant digital equipment containing personal data.*
    d. For most practices their CCG will *also* be a Data Processor for the practice, and so require its own data processing contract with the practice.

    However, although GPs are supposed to have a prior written agreement with their data processor, in real life most practices have no contract with their supplier because CCGs now own and organise practice IT equipment. The CCG may only use patient data with the GP's consent, and may act as Data Processor for the GP, e.g. when they provide risk stratification data for practice populations. If either of these situations isn't covered by a written agreement/contract then under the DPA 1998 practices are already in breach of their responsibilities. Under the GDPR this omission is likely to be more actively sought out and much more heavily penalised.
11. Should have data sharing agreements with all other data controllers to whom they provide personal data
12. Carry out a **Data Protection Impact Assessment (DPIA)** (see Article 35 & 36 if any high-risk processing (e.g. providing *identifiable* data for research) is being undertaken. This is unlikely to apply to many individual general practices. However, it would be wise to

[16] In reality this is likely to be the date at which the GDPR comes into force.

[17] In real life CCGs now procure and own most practice IT equipment and software, but, as the data controllers, *practices* must sign the data processing contracts, not the CCG, although the CCG may *arrange* the contracts.

[18] It is not clear whether GPs and hospitals need to have contracts in place: assuming that the processing is part of the patients' direct care we think they may not be required. We will all need to await further information on this point.

check whether recipients of patients' data — e.g. organisations the patient is referred to, research bodies, etc. — further disclose identifiable data to others.[19] One candidate for a DPIA could be the sharing of patient records with the patient him- or herself or his or her non-professional carers, because of the risk of infringing the data protection rights of others mentioned in it, such as third parties and family members.

13. **Update all policies in line with GDPR requirements** (once we know what these are!) Training is key, especially for new staff, those working off-site, and home workers. (Changing the culture is a lot harder.) Training needs to be *documented* and repeated at regular intervals.
    Don't forget that the GDPR applies just as much to paper-based records, audio records such as dictation tapes, recorded telephone conversations[20], pictures, video and documents being transported (such as notes in the back of your car or being worked on at home). Visitors, such as those maintaining practice premises and equipment, trade reps, etc, should also be made aware of the need to keep to themselves information they observe or deduce about patients and staff during their visit(s)[21].

Once data sharing is taking place[22], the following principles will need to be observed:

14. **There is a legal requirement to keep records of data processing activities.** However, this is another area that is currently not well-defined, and therefore where we can and should expect national guidance. It probably only applies to data disclosed on legal bases other than those given in Article 9(2) h-j, but we need to be certain of this. We also need to be informed of what each type of data processing activity record should contain.
15. **There is a legal requirement to self-report breaches, both to the ICO, and to the affected person(s), within 72 hrs of its discovery.**
16. Note that in most cases, practices now *cannot* impose charges for providing copies of records to patients or staff who request them. The requested information has to be supplied *within a month, though extensions can be negotiated for complex cases*. However, practices can charge a reasonable[23] administrative fee for a request for information if the request is unfounded or excessive.
17. There are specific requirements for transparency and provision of fair processing information to all practice data subjects (i.e. staff and patients).
18. There are tighter rules where consent is the basis for processing, e.g. for sharing patient data with others for purposes other than those explicitly permitted by GDPR. The consent must be informed, *explicit* and recorded.

[19] These impact assessments must be carried out even when a hospital is dealing with the information — in some cases a data-sharing agreement may be necessary and a DPIA is intended to ascertain this.

[20] Patients will need to be warned about these, and to consent to them occurring, much as at the present.

[21] It may be advisable under the GDPR that they sign a non-disclosure agreement before starting work in and/or on behalf of the practice.

[22] Again, in practice this is likely to be the date at which the GDPR comes into force

[23] No upper limit has been mentioned (as yet).

19. There needs to be 'Privacy by design' over future practice working — not just for IT but also the paper and manual aspects of practice work. Data protection issues must be addressed in all information processes. Don't reinvent the wheel – scope GDPR into work streams and future-proof ongoing projects.
    (Again, central guidance for general practice, integrated working, and the whole clinical and administrative NHS is needed here. It will save large amounts of practice time and, as importantly, help ensure consistent data protection behaviour across all practices.)
20. Under GDPR Article 5(1)c, practices may share only information which is relevant for stated purpose(s). The same duty was created by the DPA 1998, so this is nothing new — though more likely to be policed/penalised[24].
21. *A*ll data handling or processing actions involving identifiable data, other than for in-house patient care should be documented. For completeness' sake and to avoid confusion, it would be wise to do the same for all non-identifiable individual-level patient data that is shared outside the practice.
22. **Dealing with errors in the record. Although in other areas of data handling the subject can exercise a 'right to be forgotten' this is specifically ruled out for healthcare data. Patients do *not* have the right to request that information in the record be removed, or altered simply because the patients they don't like the implications, or disagree with the clinician's opinion.** Diagnoses can change over time as more information is received, or the progression of the disease makes the diagnosis clearer; medical opinions also change with time.
    Clearly, if there is an obvious error, the practice will want to ensure that the record is corrected, *but this must be done transparently, so that it is clear to everyone what the record previously said and when the change was made.* The reputation of those attending the patient, or their defence against a charge of clinical negligence, may rest upon whether at a particular time or date a specific diagnosis or observation had or had not yet been made.
    If you need to investigate a particular request for a change in data recording, you will need to ensure that the record isn't used for data processing while this is being done.

Security is also part of the process

23. Remember, 'read access' to information is potentially dangerous.
24. Check third parties for their policies and processes.
25. It is probably better to talk about 'information security' rather than 'cybersecurity', which is only part of information security.
26. Keep staff updated — especially on security issues such as phishing, backing up, locking doors, desks and storage areas, and removing smartcards from computers. (But note that security under GDPR is actually quite subjective and local.)
27. Raise awareness with staff of the devious human ways (as opposed to IT mechanisms) in which confidentiality can be broken — e.g. the member of staff who is conned over the

[24] This is another grey area which will be difficult to perform with present GP-related software and processes. Presumably whole record sharing would have to appear in any Fair Processing Notice for patients (see footnote 9 in section 4). Under the DPA 1998 the ICO has taken a pragmatic approach to enforcing the minimisation principle.

phone into 'trying to be helpful' by supplying information; or when someone puts a notice on a door that should be locked saying 'lock broken, security informed, please leave this door open'. Watch Facebook and what gets published there; and be aware of people mingling with your staff outside your premises for a smoke when they don't actually work there.

28. Talk about 'Raising awareness' rather than 'educational training'. This will be a continuous ongoing process.

7. Risks and burdens for practices

1. The burden of recording how and to whom data has been disclosed for multiple different purposes.
2. The increased ability of patients to access information in their record, and to ask a not-for-profit organisation to act on their behalf, which reinforces the need for manual checking by the practice of released/shared record entries to be certain that third-party or other restricted information isn't available to the recipient.[25]
3. Both 1 and 2 lead to ongoing resource implications (workload and financial), with consequent effects on patient care.
4. A specific problem is that of dual, joint liability, though this is not new. It is for the Data Controller to tell the Data Processor what should or should not be done with specific data. The GDPR makes it clear that a processor is responsible for any processing he/she/it does that the data controller didn't ask them to do (see Article 28(10).
5. The difficulty of establishing whether current mission-critical data sharing systems are permitted by the GDPR, in particular by the 'data minimisation' rule, which states that only data relevant to the recipient's purposes should be shared.
6. *The risk of not being able to complete the necessary administration documentation and introduce the new and revised procedures, contracts and agreements before the introduction of the DPA 2018 on May 25th this year…*
7. *…and therefore possibly incurring the potentially much larger fines under the GDPR*, see 3.12**.**

8. Wider concerns — for GPs, provider organisations, CCGs and CCG-practice relationships

1. While some of the preparations for the GDPR could (and should) be done once for primary care as a whole, in order to ensure consistency across the UK, *no-one has yet accepted responsibility for the task*, which amounts to preparing what the GDPR calls a "code of practice" — see Article 40 — for general practice**.** We are also concerned at the lack of national guidance from NHS management, who are best placed to set up agreements or provide templates which will be needed for smooth and uniform implementation of GDPR.

[25] Patients also need to be made aware that if they share their record with family members, carers, etc., it will contain all the data they have also asked to be 'kept private', i.e. not to be shared outside the practice, and that data provided by third parties must only be shared with the consent of the third party (we think this does not apply to other clinicians caring for the patient, as they owe the patient a duty of confidentiality). Unfortunately, most (all?) GP systems do not indicate in a computable way that data has been provided by a third party.

2. One underlying concern is that practices might be reassured by a relevant NHS body that there is no need for concern or action on the part of the practice itself, only for the practices to find that detailed and comprehensive action hasn't actually been taken by that body, leaving practices high and dry, with NHS management hiding behind the view that 'you're the Data Controller and it's up to you to be satisfied with the arrangements *before* you do any sharing'.
   There are two aspects to preparatory work done by others:
   a. The preparation of advice, guidance, forms etc
   b. The hands-on work of establishing contracts/letters of agreement with third-party providers of data processing services.
   Our feeling is that practices would be ill-advised to *assume* that other bodies have done any preparatory work needed.[26]

3. These onerous duties, reduction in remuneration, short timescales, complexity of the law, and uncertainty about duties in individual cases, all coupled with potentially huge penalties will make it likely in the opinion of at least one of us that individual practices may be reluctant to share any information at all where there is a risk of incurring a fine by contravening the GDPR. Although it is a professional duty to share information appropriately (as part of the Caldicott II guidelines) and therefore a professional offence under the GMC regulations not to do so, it is much easier to prove an action of commission by comparison with an act of omission. It is also worth re-emphasizing, by comparison with the previous regulations, that an offence is committed under the GDPR if detailed processing arrangements are demonstrably not in place and/or their application not recorded, *even if no data has been leaked.*

4. Practices need to be aware that even if they share pseudonymised data with others, it may be possible under some circumstances for the recipient to re-identify them. This possibility should explicitly either be forbidden (or allowed if required) in the relevant contract or data sharing agreement.

5. Although the ICO is being helpful, things are moving slowly: there is a twelve-point plan for readiness currently being recommended. https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

6. From a practice point of view the IG toolkit no longer becomes a tick-box exercise but something that can be used to prove they followed guidelines should there be a query in the future. The IG toolkit will require considerable (and urgent) revision in the light of the GDPR: but who is tasked with doing this, how, and when?

7. It is still not understood by everyone that when consenting to share the SystmOne record, *all* the parts of the record the patient has allowed to be placed in her 'pool'[27] are shared, not just the parts that are relevant for that setting. This also needs to be made clear to patients when asked to share their record with another SystmOne organisation. Both this, and the availability of requesting at the time very confidential information is provided that it is not shared outside the organisation it was given to, need to be made clear to all new patients, and in Fair Processing Notices displayed in the practice.

[26] Equally practices should be prepared for other organisations to assume that practices have done no preparatory work. There does need to be a joined-up and pragmatic approach here. Organisations (including practices) could find themselves needing to create and manage hundreds of agreements.

[27] For more detail on what does and what does not go into the 'pool', and where and how this pool can be viewed (or prevented from being viewed) please refer to Section 5.

8. There is also the inappropriate habit of sharing/duplicating all information on a family across all records of that family. For example, Social Services might send a single letter talking about a whole family, and the community team puts a copy on each member of that family's individual record without removing the third-party references — again, an example of how other organisations don't understand the rules. The ability to easily put a letter on each record means it's done and forgotten about. This is an illegal action now[28]: it will be just as illegal (but more expensive) if done in the future. (And it may not be the practice's fault, but as one of the Data Controllers in common it will be in part the practice's responsibility — compounded by the obligation to destroy Social Service records in most circumstances 3 years after reaching maturity.) We are not sure what penalties this might attract after GDPR – especially as the Community organisation which made the entry (and the only one that could remove it) may well no longer exist

9. What recommendations should the profession (BMA, LMCs, CCG, FCI, PHCSG etc) be making to government and to statutory bodies?

1. General practice urgently needs a source of central authoritative guidance on exactly what practices need to do to implement the GDPR (BMA/BCS/DH/NHS England, NHS Digital, the ICO).

2. Similarly, there needs to be *detailed guidance on what the protocols and records of data processing activity should contain*, together with *detailed guidance on exactly whom/what situations these should apply to.*

3. CCGs and hospitals must be required to confirm to primary care practices (easily and transparently) that their own procedures comply with the GDPR.[29] The reverse also should apply.

4. CCGs must be required to confirm to practices that the CCG's duties under the law have been completed (and indeed, what exactly these duties are).

5. Government needs to be aware that there is disquiet among ordinary general practices[30] about the problems which are likely to arise after the inception of GDPR.

6. There needs to be an urgent examination of whether the single shared record as currently implemented is permitted under the GDPR, and if it is not, how it may be enabled.[31]

---

[28] Though there is a public health requirement to maintain family records, so this is another example of conflicting rules and practice.

[29] This needs to work both ways. Practices need to be able to assure provider organisation that they are compliant, have training and policies/processes in place. Historically, many significant data breaches have been where practices have shared other organisations' data inappropriately with third parties, causing significant harm.

[30] And provider organisations — indeed, across the entire NHS!

[31] Please note that this suggestion is *not* intended to imply that using a single shared record (e.g. SystmOne) is currently illegal. We are of the opinion that its use is covered through appropriate use of the separate mechanism of consent (see Section 5, footnote 11 on page 8 of this document). Our request therefore is that ultimately the unique circumstances of the single shared record will specifically be covered within the GDPR itself.

7. In addition there needs to be an examination to see if other data sharing models used by general practice systems are permitted by the GDPR, and if not, how they may be enabled.

8. There is uncertainty over the size of any initial penalties issued under the GDPR: will they be hefty in order to 'make a point', or minimal, in recognition of the running-in period that the GDPR will inevitably need? We believe strongly that the latter is the more sensible approach, especially in the light of the short time UK data controllers (e.g. general practices) and processors (e.g. GP system suppliers) have to become familiar with, and then implement, the GDPR, and also the lack of official guidance that has been given in some subject areas.

9. There needs to be official recognition that that general practice may not be able to complete the preparations needed to properly implement the GDPR by the 25th of May, and measures should be put in place to at least delay the issuing of fines for non-compliance.

10. Recognition needs to be given over the resources involved when practices provide copies of the notes for legal or insurance cases — especially photocopying paper notes (when the practice is non-fully electronic, as is often the case); and also the immense amounts of scarce practice time spent sifting through every piece of paper (real or virtual) to ensure there are no third party references. The GPC needs to become involved here, as the loss of money/staff time can be enormous: it is not appropriate that the GP should have to subside legal processes.

11. Clear and unambiguous limits need to be created and publicly stated over the exact size of the record beyond which copying/extracting the records is deemed to be excessive. This will define the record size beyond which the practice can both charge for the time taken to vet the record, and have an increased time-limit to complete the work. A clear statement of the amount practices are allowed to charge is also needed.

Appendix: Further links and reference material

The Final version of the Regulation, released 6 April 2016:
http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

The Information Governance Alliance (IGA) "CEO Briefing Note. Changes to Data Protection Legislation: why this matters *to you*" is very helpful and commendably pithy. It can be found at https://digital.nhs.uk/article/6921/Changes-to-Data-Protection-legislation-why-this-matters-to-you.

NHS Digital has a large collection of documents and guides at https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

A general set of descriptors/FAQs, etc: http://www.eugdpr.org

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

The BMA and the Information Governance Alliance (IGA) have now produced more detailed guidance.

The latest BMA guidance ("GPs as data controllers under the General Data Protection Regulation" - published March 2018) gives details on "Consent and other lawful bases for processing".

The IGA has produced some guidelines on *Consent* https://t.co/bA2MyPFOOL and *Guidance on Lawful processing* https://t.co/A6btbosIgT .