GDPR Guide for Spire Consultants, GPs and AHPs and their Medical Secretaries

This guide provides general information on GDPR compliance as at 1 May 2018. It should not be relied on as legal advice. You should take your own professional advice based upon your specific circumstances.

30 April 2018
Version 1

Contents

Section A - Background

On Friday 25 May, 2018, a new law relating to personal data comes into effect that radically changes some of the requirements concerning data protection. The new law, known as the General Data Protection Regulation (GDPR) will impact:

- every consultant's entire private practice, where they will be responsible for ensuring compliance; and
- every consultant's relationship with Spire (and other hospitals that they practice at), where consultants will be jointly responsible with each provider for ensuring compliance; and
- every medical secretary's administrational activities, as they will need to implement some key changes and in many cases also ensure compliance in certain areas.

A.1. Why is GDPR important to you?

Healthcare has recently been of interest to the regulator, the Information Commissioner's Office (the ICO) because of some well-publicised security breaches affecting public and private providers and the increasing incidence of third party attacks on information systems. GDPR contains requirements which directly impact the patient journey, medical records management, referrals, research and data sharing activities and the introduction and use of new information systems or services. The requirements will become part of healthcare's legal landscape and will be enforced by sector and professional regulators.

Self-employed consultants, GPs and Allied Healthcare Professionals with practising privileges (collectively referred to in this guide as "consultants"), medical secretaries, PMIs and all hospitals will all be impacted directly by GDPR.

The key principles around data handling are not affected by GDPR – the new law is an evolution not a revolution - but healthcare data security remains a key concern. Healthcare data was previously called "sensitive" personal data and under GDPR is now "special category".

GDPR restates existing UK data protection law and adds strict new rules on the handling, processing and protection of patient and other personal data, whether held on paper or on IT systems. It applies to anyone who determines the purposes for which personal data is collected or used – known as ***"data controllers" (DCs)***. Consultants will usually be DCs because they exercise decision-making and professional judgement in regards to collecting and using personal data. For the first time it also introduces direct compliance obligations on those who process personal data on a DC's instruction (such as a payroll service or usually a self-employed medical secretary) – known as **"data processors" (DPs)**. See Annex 1 for details.

The new law introduces new rights for individuals, including new rights of access to and control over their personal data. This includes patient data which is held and used by you and Spire.

GDPR covers the use of all personal data relating to a living individual for non-domestic contexts: patient, employee and marketing and business development data are all impacted. All patient-identifying data is "personal data" (which also includes any identifiers which have the potential to identify individuals (e.g. a patient's NHS number)) and as such is covered by the GDPR requirements. This means that the requirements will usually apply equally to **pseudonymised data** as to more clearly identifiable personal data, so it should be treated in exactly the same way.

The ICO also has new powers to audit, investigate and to restrict processing.

GDPR should be welcomed as a motivator for companies in our new digital age to significantly increase consumer (patient) trust by strengthening organisational responsibility and developing robust evidenced based governance and compliance. Communication, clarity and transparency will be improved and adherence to best practise more visible.

There remain some practical challenges, including the fact that the UK government has not passed the new data protection act yet which will put some UK specific provisions in place around GDPR. This is all without considering Brexit (see D1).

A.2. The financial impact of GDPR

A key GDPR requirement is that you can demonstrate compliance with the new law.

GDPR introduces increased powers for the ICO, including higher levels of fines for non-compliance (the maximum under current law is £500k and this will increase under GDPR *to **4% of turnover or €20m - whichever is higher***). Any DC or processer can be fined by the ICO for a breach. Both DPs and DCs may also be liable for breaches and resulting civil claims for compensation. Claiming compensation will become easier under GDPR.

Both DCs and data processes should consider the impact of these new commercial risks and consider reviewing insurance cover for data issues.
(See FAQ D.2.)

A.3. How does GDPR affect your relationship with Spire?

GDPR makes clear that consultants will be "DCs" over various categories of data including data relating to their patients. In some circumstances, consultants will be jointly responsible for compliance with hospital providers and other third parties.

This change in law is something that impacts us all, with no exceptions. Spire is taking the change in law very seriously and has a dedicated project team which is working hard to achieve compliance for Spire and also to help smooth the path for its consultants and their medical secretaries in particular.

Joint responsibility

Under GDPR, both Spire and consultants will be DCs and will be responsible for protecting their patients' personal data. They will be treated as **joint data controllers** in respect of any Spire patient data and will be jointly responsible with Spire for ensuring compliance under GDPR. In other words, they will be jointly responsible for the way the data is processed and protected. In addition, the new law enables a patient to complain (and claim) in relation to the use of their data against either Spire or the consultant.

GDPR requires that:

"***joint data controllers*** *… shall in a transparent manner determine their respective responsibilities for compliance..."*

Given this, Spire will be putting in place a **mandatory Data Sharing Agreement and Data Rules** setting out how Spire and consultants will act to protect Spire patient personal data (SPPD) in compliance with the new law and laying out a matrix of data responsibilities. There will be no need to sign the Data Sharing Agreement or Data Rules: they will be a condition of practising at Spire.

GDPR will affect private practice outside Spire in the same way, but the data sharing and other arrangements we are establishing will only apply to a consultant's Spire patients: broadly speaking, these are patients who have enquired about care at a Spire facility, or have been referred to Spire or have been booked or registered with Spire AND any of these activities are linked to a consultant.

Another particular area to focus on is "data processing". Self-employed medical secretaries, or services companies, who provide patient administration, typing, document preparation and medical record services to consultants are usually data processors. Spire's medical secretary provision is therefore a DP relationship and we will be putting a contract in place (provided by the Spire GDPR team) with all consultants who use Spire employed medical secretaries (Spire MedSecs), to meet new requirements.

Finally we will provide a privacy notice to consultants which covers how Spire treats the data that Spire holds about them.

A.4. <u>What is Spire doing to help you with GDPR?</u>

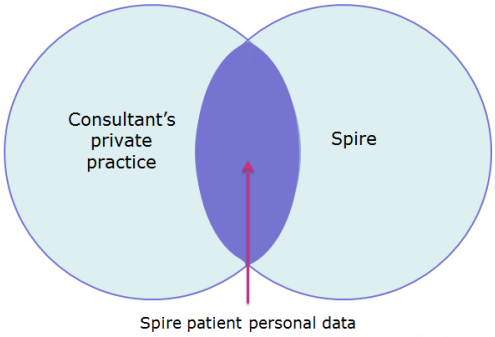
GDPR will impact:

- every consultant's entire private practice, where they will be responsible for ensuring compliance; and
- every consultant's relationship with Spire and other hospitals where they practice, where consultants will be jointly responsible with each provider for ensuring compliance; and
- every medical secretary's administrational activities, as they will need to implement some key changes and in many cases also ensure compliance in certain areas.

Spire patient personal data (SPPD) (see Figure 1 below) is the set of data that Spire and a consultant is jointly responsible for and that this guide covers. Spire patients not linked to a consultant (e.g. physiotherapy patients or patients at the early stage of an enquiry who have not been referred a particular consultant) are not covered. Nor is a consultant's private practice with other providers. Consultants will find though, that much of the help, as described below and in the remainder of this guide, that Spire is providing to help them with GDPR compliance for SPPD, will also help them significantly with their wider practice.

This guide covers consultants' private practice at Spire – that includes both the private and NHS patients treated with us and it also provides information on obligations in relation to their wider private practice.

Figure 1: Spire Patient Personal Data



In order to make preparing for GDPR as easy as possible, Spire is doing as much as we possibly can to smooth your path to compliance:

Example/model documents for consultants. As well as this guide, we are providing detailed worked examples of key regulatory documents that are needed for compliance in private practice. We have ensured that any data processing done by consultants and medical secretaries for Spire patients is covered in our privacy notice. This, where consultants only practice at Spire, may mean that they do not need to issue their own (see B5 and D4). Also, for all data processes that are undertaken by Spire, our compliance documents can be referenced e.g. our record of processing (see B3) which should materially reduce the complexity of what must be prepared. We are also providing a Data Sharing Agreement which meets the joint regulatory responsibility to detail our respective accountabilities with consultants for SPPD. For those consultants using Spire MedSecs, we will put in place with you the required data processing contract (see B6).

All the documents mentioned above are explained in detail in the relevant parts of Section B of this guide and the examples will be provided on our website at www.spirehealthcare.com/gdpr .

Spire documents: To help consultants comply with their security requirements, we have created a set of Data Rules that will form part of the Data Sharing Agreement that outlines the requirements for consultants, medical secretaries and Spire staff to follow when processing SPPD. This will help you to ensure that you meet GDPR security requirements, although you should take you own advice. In addition, Section C of this guide focuses on security and there are many practical suggestions and FAQs about how to tackle key security issues.

Spire will also provide consultants with our updated data protection and information policies when they are completed in mid-May. These may be helpful when you are creating your own policies.

A consultant who only practices at Spire, has a Spire MedSec and operates a secure, paperless practice, will probably find that they have little extra to do to achieve compliance. Spire will be able to provide the consultant with the majority of the documentation this is required to meet the regulatory requirements. Some documents may require some minor amendments to tailor them to the specifics of the practice but this should not be onerous.

Spire's proposed IT services: Spire will be providing a photography app (see C.4) and is investigating the provision of a data storage solution (see C.8 (A)) A consultant app is already being rolled out (see C.8 (A)).

Single patient record: Finally, in order to simplify our joint response to patient requests for medical records, to increase the security and availability of patient information and to meet CQC requirements, Spire will be finalising the roll-out of the single patient record during 2018.

Electronic access to SPPD: We are also commencing a project to implement an electronic patient record. We are already rolling out a consultant portal (accessible by consultants and medical secretaries) across the Spire network that materially reduces the need for other forms of communication between medical secretaries and Spire. Not only can all patient administration details can be viewed remotely but also bookings can be made electronically. Please ask about access to the consultant portal at your hospital. Where the portal is not yet available, an earlier version, known as "clinic viewer" can be used instead. The final piece in the electronic offering is the patient app, which is currently under development. This will allow patients to access a variety of information online, again reducing the need for some information flows to be managed by Spire staff or medical secretaries.

All our GDPR documentation will available at www.spirehealthcare.com/gdpr . The website will detail expected release dates of documents not yet available. In addition, video recordings of our GDPR seminars will be made available.

Section B: 10 things the GDPR law requires DCs to do….

This Section B outlines the main requirements on DCs of personal data and what DCs should be doing now to prepare for 25th May, 2018.

GDPR implementation checklist:

1. Understand you classification as a DC or a DP
2. Pay a fee to ICO
3. Maintain a record of processing
4. Create a written data inventory as part of your record of processing
5. Decide whether you need a PN, and if so create one and make it available to patients and/or staff
6. Identify your data processors and make sure you have a compliant contract
7. Ensure you are processing data lawfully
8. Audit your security arrangements and data protection policies
9. Create a compliance plan
10. Create your policies and processes for data subject rights and breaches

Some GDPR compliance requirements, such as information security rules, apply to everyone handling patient data including medical secretaries as DPs. Spire's data security rules are detailed in Section C.

B.1. Understand your classification as a DC or a DP

Identifying whether you are a DC, or a DP, or neither, is key to GDPR compliance – obligations are different for DCs and DPs. ***A controller*** *"determines the purpose and means of processing".* This means for example anyone who decides which data to collect, how and why it will be used and stored and how long it will be held for. The ICO's guidance is that professionals exercising their own judgement about their services will usually be DCs, as will those who interpret or materially alter data and those who ***exercise professional judgement or decision-making*** in relation to data. In the light of this, Spire's view is that all self-employed consultants (including radiologists and

anaesthetists) with practising privileges at Spire are DCs. In addition, all self-employed GPs and AHPs with practising privileges are DCs.

Self-employed medical secretaries are usually DPs acting under instructions from their consultants. Corporate entities providing medical secretary services are usually DCs (not least in relation to their staff) and should seek advice. Such entities may be DCs in their own right, due to certain services that they provide and in relation to the staff data that they hold but for the services that they provide to consultants, they are likely to be acting as DPs.

If you are a self-employed consultant, it is your responsibility to carry out the regulatory tasks covered in this Section B of the guide, including putting policies in place and training your staff.

If you are employed by a large corporate entity such as Spire, that **entity will be the DC** and will be responsible for carrying out the regulatory tasks covered in this Section B of the guide. Any of its employees who are processing SPPD must follow their employer's data protection policies and Spire's Data Rules.

If you are employed by a small entity, partnership or other structure, the position will depend on the exact nature of the arrangements and you should take expert advice.

The same principles apply to medical secretaries as DPs – please refer to Annex 1 for the DP obligations under GDPR.

There may be exceptions to the above categorisations. The ICO has provided helpful guidance on the difference between DCs and DPs. If you are not clear, please refer to Annex 2 for more details.

B.2. Pay a fee to the ICO

Under the current regulations, consultants as DCs) are required to register with the ICO. GDPR removes registration requirements, but the Government intends to put in place a fee scheme requiring all DCs to pay an annual fee to the ICO. Only DCs will be subject to the fee, so medical secretaries will not need to pay, as long as they are solely DPs.

The ICO has produced a guide to the new data protection fee, based on draft legislation.
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/guide-to-the-data-protection-fee/

The lowest level of fee is expected to be unchanged from the current position: £35 if DC turnover is less than £632k where the fee is paid by direct debit.

From May 25th, the Spire hospital management team be checking evidence of each consultant's payment to the ICO as part of the annual review.

B.3. Maintain a record of processing (and DPs)

Each DC "shall maintain a record of processing activities under its responsibility".

- This up to date written record must show:
    - name and contact details of the DC, it's representatives and it's Data Protection Officer (DPO) (if a DPO is required)
    - purposes of the processing (this includes storage – see B4 on storage below)
    - categories of data subjects and data
    - categories of third parties (as described below) to whom the DC has transferred or may transfer data
    - identity of third party international organisations that data is transferred to and suitable safeguards. (Spire does not permit transfers of data outside the EEA (apart from to referrers or patients with their consent) except with the permission of Spire's DPO.) (See Annex 3 for further details on GDPR requirements for international transfers and storage)
    - where possible, envisaged time limits for erasure of each category of data
    - where possible, a general description of technical and organisational security measures

- Third parties may include: any medical secretaries not employed by the consultant, companies providing secretarial or transcription services, PMIs, GPs, LLPs, other consultants, other healthcare professionals, clinical equipment providers, research companies, IT providers, email providers, transcription services, billing companies and debt collectors.

What is Spire doing to help you for Spire Patients?

- The Spire record of processing will cover data processed on Spire-managed equipment by Spire staff including Spire employed medical secretaries, **so your record of processing can reference the Spire record** for this part of the practice. Your record should cover anything outside the Spire part of the private practice (e.g. data processing for all non-Spire patients and data processed or stored on the consultant's or medical secretaries own systems or premises.
- **Spire will provide an example record of processing** on our website www.spirehealthcare.com/gdpr . This is also useful for the non-Spire part of the private practice.
- If a consultant has a Spire employed medical secretary and a secure, paperless private practice solely at Spire, we expect that the of record of processing will be a very short document but we still recommend having one, just in case the ICO knocks on the door.

B.4. Create a written data inventory (and DPs)

DCs and DPs will struggle to comply with GDPR if they do not understand what personal data they hold, where it comes from and how it is handled (or transferred to others). Many create a data inventory in order to manage their data obligations. For those with limited personal data holdings, this might be combined with the record of processing (see B.3.).

A data inventory supports a data minimisation and data retention programme: GDPR puts a new emphasis on the minimisation of personal data holdings (only what is necessary) and the period of personal data holdings (only for so long as necessary). This incentivises DCs/DPs to document their reasons for retaining personal data.

The data inventory (e.g. a spreadsheet) should cover:

- What types of data you store
- Why you store it
- Where and how the data types are stored e.g. on paper, electronically, email, clouds or other systems
- Storage by third parties e.g. email and IT providers and self-employed medical secretaries
- How the data and storage devices are secured (see Section C)
- Any international storage (including cloud and email providers) See Annex 3

DCs must also ensure they have a written data retention policy and comply with it and ensure their DPs do also. Spire is adopting a 30 year retention policy for all medical records. The NHS policy employs different timeframes which you could also consider.

What is Spire doing to help DCs and DPs with Spire patients?

- Spire's data inventory covers data stored on Spire premises and Spire managed equipment by Spire staff including Spire MedSecs. Your inventory can reference the Spire inventory for Spire patients. You should record in your data inventory any other places where you hold SPPD. Your non-Spire patients should also be covered in your inventory.
- Spire will provide an example data inventory on our website www.spirehealthcare.com/gdpr. This is also useful for your non-Spire patients.
- If a consultant has a Spire MedSec and a secure paperless private practice solely at Spire, we expect the data inventory will be a very short document but we still recommend having one, just in case the ICO knocks on the door.

B.5. Provide patients with a privacy notice

- DCs are required to provide patients with a notice that sets out how their data is collected and used. This is called a Privacy Notice (PN) or a Fair Processing Notice. Extensive detailed requirements are specified for the content and format. (See D3.)
- Privacy notices need to be sensitive to their audience and concise, accessible, easily intelligible and in clear and plain language. This is quite challenging to achieve in the context of the quantity of specified contents. Privacy notices may need to be addressed to minors, and be easily understood by them.
- A PN is only required if and when DCs collect or process data – they are not required for patients if no data is written down on paper or recorded electronically (on an IT system or by a voice recording on the telephone).
- For all patients under 18, DCs should provide the adult PN to the parent/guardian. For patients between 13 and 18, DCs must also provide a child friendly PN.

What is Spire doing to help DCs for Spire Patients?

- Spire will have an adult PN and a child friendly one that covers SPPD but only for the purposes of their direct clinical care with Spire. Spire will signpost patients to the Spire PN as soon as practically possible during or after their first point of contact with us.
- **In order to be covered by the Spire PN**, consultants/medical secretaries booking patients into Spire or collecting data from patients who have agreed to be treated at Spire, must refer the patient to the Spire PN during the email exchange or telephone conversation, as appropriate, and in the appointment letter. (See example wording and further process details in FAQ D4.)

- **DCs will need their own PN to** cover other circumstances e.g. early stage enquiries from patients from whom data has been collected, who are going to attend a non-Spire hospital, or where the provider is not yet confirmed. In response to requests from consultants, **Spire has created an example PN** that maybe adapted and used as appropriate. This is available at www.spirehealthcare.com/gdpr. We are also investigating whether **Spire can host consultants' own PN** on the consultant's individual webpage on the Spire website.
- Consultants who practice solely at Spire and have a Spire MedSec should not need to have their own PN, as all patients will be processed jointly by the consultant and Spire from the patient's first enquiry. In this case, if consultants have a website that takes enquiries or bookings, patients should be signposted to the Spire PN by a link from the consultant's website.
- I**f a Spire MedSec is processing data for patients who are being treated at other providers,** the consultant must ensure that either their own PN or the other provider's explains to the patients that their data may be processed by Spire (or e.g. another hospital provider).

B.6. Update or establish third party contracts

GDPR requires that DPs provide "sufficient guarantees" that they have implemented sufficient measures to comply with GDPR. The ICO's guidance confirms that DCs have a **responsibility to check that any DP is competent to process data in accordance with GDPR**. The law also requires that any data stored or processed for DCs by a third party is covered by a **written contract** that controls the way the DP conducts their tasks and ensures their GDPR compliance. The GDPR specifies a detailed list of contents. DCs should audit their third party contracts (and DPs should review theirs too). Spire is doing this - it's a massive task!

- See B.3 for examples of third parties. (See D.10 re DGL/Clanwilliam).
- In order to comply, Spire will be putting in place a DP contract for the provision of medical secretary services by Spire to consultants. The contract will be provided by Spire's GDPR project team.
- Those employing medical secretaries should ensure the employment terms comply with GDPR and protect both parties (see D.5).
- Those using a third party medical secretary (who is not employed) should have a service contract in place with them (even if it is your wife/husband!) and this must include a GDPR-compliant data protection clause.
- See Annex 3 for further details on the stricter GDPR requirements for international transfers and storage and Spire policy
- **Spire has provided a model GDPR compliance clause** as an example of the sort of provisions one would expect in a DP agreement to ensure GDPR compliance. It is available on the website www.spirehealthcare.com/gdpr.
- The ICO's guidance is available https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf .

B.7. Understand the legal basis for the use of personal data

Under GDPR, personal data use must be:

- fair
- lawful
- transparent
- based on a specific "legal basis" – one of a limited set of bases set out in GDPR.

Fairness is not specifically defined, but implies a "good faith" approach to data use and the balancing and consideration of individuals' interests against those of a DC.

Transparency includes the notification and related communication obligations on DCs (see B.5).

Lawful use requires compliance with any applicable law relating to the activity or data in question. In healthcare, the most obvious is the law on patient confidentiality and consent to treatment.

The ***legal bases*** for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever personal data is processed. They are:

- **Consent:** the patient has given consent for the processing of their personal data. Consent must be a clear, informed, recent, specific opt-in
- **Contract:** the processing is necessary for a contract with the individual, or because they have asked for specific steps to be taken before entering into a contract
- **Legal obligation:** the processing is necessary to comply with the law
- **Vital interests:** the processing is necessary to protect someone's life
- **Public task:** the processing is necessary to perform a task in the public interest or for the DC's official functions, and the task or function has a clear basis in law
- **Legitimate interests:** the processing is necessary for the DC's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data (which overrides those legitimate interests)

In addition, where the personal data relates to health, an additional specific legal basis must apply. The most relevant of these for Spire and consultants will be:

- The provision of healthcare
- "Explicit" consent
- Protection of the vital interests of an individual where they cannot consent (such as emergency medical treatment to an unconscious patient)

The usual processing basis under GDPR in private healthcare settings is the performance of the contract for healthcare plus the provision of healthcare to process the health related data.

These bases also cover communications between the clinical team directly providing the care and those supporting them for administrational purposes (such as medical secretaries and billing) and all their communications with the patient. Local clinical audit is also covered by legitimate interests.

In order that such healthcare is lawful, confidentiality and consent to treatment rules must also be followed: GDPR does not affect the law on lawful consent to treatment for patients which is covered in detail by the GMC Guidance on Confidentiality https://www.gmc-uk.org/-/media/documents/confidentiality-good-practice-in-handling-patient-information---english-0417_pdf-70080105.pdf . The guidance has recently been updated for GDPR and is very helpful about consent and disclosure. Also see: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf.

- The GMC Guidance explains that processing data to do things **necessary** to provide direct patient care (e.g. the creation or storage of medical records, communications containing personal data between the care team (including medical secretaries) and billing) should not require specific patient consent. (See D.6).
- Consultants should obtain explicit patient consent for any onward referrals to another consultant and this should be documented. This consent combined with the PN also

covers the transfer of any relevant clinical data. Data being transferred to referrers and GPs is covered in the Spire Privacy Notice (see B5 above).

- Consent for minors. See B5 above.
- Using patient data for any reason other than direct care (and the support thereof) such as marketing, promotion (e.g. before and after photos) or outcome data is **likely to need GDPR compliant consent**. Sharing patient data with r**egistries** will also need explicit consent unless it is a legal requirement. Most registries have their own consent process.
- The GMC also recommend that consultants obtain explicit written patient consent to use their data for **research** (unless there is Section 251 approval under the NHS Act 2006 and it is not practical to gain consent (not Scotland)).
- Historical consents should be reviewed for compliance: the experience of many businesses is that historical consents are inadequate and that new consents need to be taken if the information is to be retained.
- Sharing data **with insurers (PMI)**: we are reviewing the circumstances under which consent is required to share patient data with the insurer funding the treatment and will provide an update as appropriate.

B.8. Process data securely (and DPs)

- **Audit your security practices** and ensure you are storing and processing data securely and in compliance with GDPR, Spire's Data Rules and applicable codes of practice issued by regulatory and advisory bodies such as the BMA, GMC, CQC or NMC.
- See Section C and security related FAQ in Section D.

B.9. Create a compliance plan (and DPs)

The law says:

"The DC shall be responsible for and be able to demonstrate compliance with [the data protection principles]"

"the DC shall be …able to demonstrate that processing is performed in accordance with this Regulation..."

Demonstrating compliance with the data protection principles is at the heart of GDPR. Enforcement action may be taken (including fines) **even if nothing has gone wrong**.

- Research a DC's obligations: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- Set out how the GDPR obligations will be complied with to keep patient, employee or other personal data safe
- Include a record of processing showing how data is used and who it is shared with
- **Have written data protection policies and procedures** in place. Spire will be updating its data protection policies in mid-May which you may find helpful when thinking about your own…
- Seek legal advice if the obligations are not clear
- Identify gaps in compliance and how they will be rectified
- Write down a plan for compliance – GDPR requires evidence of compliance and if there is a breach the ICO may ask to see it
- Keep the plan up to date

- Be aware of the need to undertake Privacy Impact Assessments for new processes with a high risk to individuals' privacy. There is a code of conduct for these on the ICO's website https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

B.10. Have processes in place for data subject rights and breaches

A. Data Subject Rights (DSRs)

Patients have new rights over their data:

- The right to be informed (usually covered by privacy notices)
- The right of access (often known as Subject Access Requests (SARs) which relate to being able to obtain copies (electronic or paper) of their data - everything from the medical record to billing data and email correspondence. You may ask the individual to specify the information the request relates to
- The right to rectification
- The right to erasure (to be forgotten).
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

DSRs are usually **FREE** including the requests for copies of medical records that providers have traditionally charged a photocopying fee for. A 'reasonable fee' can be charged based on administration costs if a request is manifestly unfounded or excessive, particularly if it is repetitive. A reasonable fee can also be charged to comply with requests for further copies of the same information. Access requests must be responded to within a calendar month. In certain circumstances it is not necessary to respond or extra time may be permissible.

The ICO has issued guidance, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ and the NHS plans to issue its own guidance on these rights. Other guidance, including the BMA's guidance titled *Access to health records* is helpful and is expected to be updated to refer to the new rules.

DSRs are not absolute, meaning that under certain circumstances the **DC may not have to comply** with the request, if they have a justifiable reason for refusing to do so (although they must respond with an explanation). For example, it is necessary for Spire to keep patient's medical records for various purposes such as managing legal claims, supporting product recalls and supporting investigations and other clinical audits relating to patient safety. Spire would therefore be unlikely to agree to a patient request for the erasure of their medical record specifically (the "right to be forgotten"). Nor would a DC be obliged erase the relevant information of data subject that owed them money.

Spire's policy on patient data rights

An overview of Spire's policy on patient data rights is included in FAQ D7 and will be included in Spire's new DSR policy that will be available by mid-May.

In summary, the Spire policy states that responding to requests for the exercise of patient data rights addressed to a consultant is the **consultant's responsibility**.

The only exception to that will be medical record requests. The new rights are relevant here but as Spire will be holding the single patient record, as joint DC, **Spire will continue to process any requests for medical records that a consultant receives**. Where the request is for other information or represents the exercise of other patient DSR rights, the patient should **be directed to Spire's DPO**.

SAR requests from law firms: Where Spire receives a pre-litigation request for copy of medical records from a law firm, we will:

- reply stating the copy charges
- charge that fee, unless the law firm responds and phrases their request as a subject access request from their data subject client

We will review this policy against market practice from our competitors after three months, taking into account our experience with the requesting law firms.

Single patient record: Given the short time frame to respond to SARs - usually 30 days, Spire will be completing the roll-out of the single patient record during 2018. The policy requires that Spire's medical record department hold a copy of all medical records and clinical correspondence including a consultant's outpatient notes. Consultants may continue to maintain their own records. The Spire single patient record may only be used on Spire premises. Having a single patient record will enable Spire to respond to SARs on our joint behalf, in a cost-effective, timely and accurate manner.

B. Breaches of GDPR

These are security breaches that lead to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data, even if only temporarily.

The GDPR says these must be **notified to the ICO** without undue delay and, where feasible, **within 72 hours** of first awareness ***if*** they are likely to result in risks to people's rights and freedoms. If a notification is later it must be accompanied by an explanation for the delay.

Breaches must also be notified to data subjects if the breach is "likely to result in a high risk" to the data subject's rights and freedoms. The ICO gives the accidental disclosure of hospital patient records as an example of the type of data breach that would need to be notified to individuals.

One of the reasons that encryption of patient data in electronic form is important, is that unauthorised access to encrypted data, where the encryption is not compromised, does not have to be reported to affected individuals.

For Spire patients:

All data breaches should be reported to the Spire DPO as soon as possible and within 24 hours at dataprotection@spirehealthcare.com and also to the Spire hospital director.

Spire will help by:

- Determining if the breach is reportable plus notifying the ICO and patients if that is required (for Spire patients)

Be aware of and comply with Spire's new documents and requirements

- Review Spire's Data Sharing Agreement and Rules and ensure you comply
- Review the amendments to the Consultant's Handbook *(these are minor)*

- Where applicable review the amended Panel T&Cs, Spire GP Engagement Letter, Self-Pay T&Cs and if appropriate, ensure they have been signed
- Spire's GDPR Project team will provide a DP contract for consultants with a Spire employed medical secretary,

Section C: Ensure data is processed in compliance with GDPR

GDPR requires that you use "*appropriate technical and organisational security measures*". This applies to everyone: DPs and DCs and their staff. There will be a balance between: nature, scope and purpose of processing, costs, technology, risk of breach and potential harm to data subjects. It is necessary to ensure that only data necessary for the purpose and its duration is processed.

In an **emergency** situation, attention should be paid to use of the word "appropriate". Complying with data protection requirements should not impede the necessary treatment of the patient. Take any data protection measures that can be appropriately taken, given the situation, and if appropriate subsequently advise to the patient.

SPPD should be kept confidential and secure and handled it in accordance with Spire's data protection and information governance policies (available from mid-May 2018) and applicable codes of practice issued by GMC or NMC. SPPD should only be accessed by people trained in data protection and who have a valid reason for access it, whether held on paper or electronic means.

Spire's Data Sharing Rules are based on the security measures detailed below. These Rules are also useful for non-Spire patients, with the exception of any references to Spire systems.

C.1. How to email securely

The ICO recommends that "*when transmitting personal data over the internet, particularly sensitive personal data, DCs should use **an encrypted** communication protocol*" and says that *"where such losses [of personal data] occur and where encryption software has not been used to protect the data, regulatory action may be pursued".*

Standard email protocol is not a "secure" method of transit for healthcare data (even if using attachments with **password protection**).

- Spire will be implementing a **new email policy** from 15th May, 2018. The key points of this policy are:
    - In our new registration form, Spire is expressly asking patients to state their preferences regarding the use of email for the two categories described below. Provided that patients have specifically confirmed their agreement in writing for each category:
        - Routine administrative emails, including basic appointment details, may be sent providing the email does not contain any more detailed healthcare or patient data (See description of basic details in FAQ D8).
        - Detailed healthcare data (such as consultation outcomes, referrals, test or diagnostic results) should be sent by encrypted email.
    - Spire requires you to check (by email or phone) **the first time you** send an important or urgent encrypted email, that the patient is able to open and access encrypted emails (unless the communication is also being posted first class).

- All **emails between organisations** and professionals (including PMIs) or professionals that relate to a Spire patient must be encrypted (unless they are within a secure network e.g. within Spire or nhs.net to nhs.net account).
- In an **emergency** situation, consideration can be given to sending emails with clinical data unencrypted (the law calls for appropriate security measures).
- If a **patients requests an unencrypted** or non-secure email for communication of healthcare data (or invoicing information), this may be done, provided that informed written consent is obtained in advance and the risks have been highlighted to the patient. Consideration should be given to other applicable security measures (the use of a password, limiting the data transferred). Security of healthcare data in transit is a DC's responsibility (Spire and the treating consultant) and the use of unencrypted email exposes DCs to risk. Exceptions should be based on a clear patient need and their understanding of the information risks; this should involve a situation specific discussion and not be a general practice. **Spire employees** will need to seek specific authorisation for this.

- Do not use **global or cloud email providers** unless you are satisfied that the provider sufficiently satisfies the GDPR requirements. See C8 for a more detailed discussion of global email providers.
- Spire uses and recommends the **Egress Switch encryption** service. (See D.9).
- **DGL:** The current DGL password email service is not GDPR compliant. DGL has recently launched an upgrade process with an encryption service that also uses Egress. This is DGL's GDPR compliance upgrade. (See D.10) .

C.2. How to manage paper securely

- Store SPPD in a secured lockable cabinet in secured premises.
- Do not leave any SPPD unattended (such as on a desk in an unlocked office).
- Medical secretaries working for multiple doctors should ensure files are only accessible by the relevant consultant.
- SPPD being handled in a public area should be turned face down whenever possible.
- Continuously accompany any SPPD carried around a Spire site without a lockable container/case.
- Transport SPPD when away from the Spire site in a secure lockable container or carrier (e.g. locked briefcase).
- Do not leave SPPD unattended in a car overnight.
- Open incoming mail and prepare outgoing mail in private areas.
- Post hard copy SPPD using Royal Mail standard post marked "P&C" or "addressee only" and send to a named addressee only.
- Dispatch items that relate to multiple patients, or are a material part of a patient's medical record or include any images, using a courier or registered post.
- Only duplicate copies of the single patient record may be removed from the hospital (with the exception of clinical emergencies).
- Spire MedSecs should not be storing medical records for patients treated at Spire at their houses or other venues. If you have records at home, please contact gdpr@spirehealthcare.com .

C.3. How to manage electronic devices and data securely

- Do not use cloud storage solutions unless you are satisfied that the provider sufficiently satisfies the GDPR requirements. See C8 for a more detailed explanation of global cloud providers.
- Files held on shared servers, including Spire's, should be access controlled so that only those trained in data protection and who have a valid reason to access it, can do so.
- Devices such as mobiles, tablets, laptops and external hard drives should be encrypted. The way to encrypt your laptop depends on the manufacturer and software package you use but it is usually quite easy and only takes a few key strokes. Try googling or find an IT service provider, or contact apple help!
- Electronic storage devices such as CDs, memory sticks and external hard drives should always be encrypted.
- Computers, laptops, external hard drives and all mobile devices should be password protected with password changes at least every 90 days. Never share or write down passwords or login details.
- Set onscreen notifications on mobile devices so they do not show SPPD.

C.4. ***How to manage photographs and dictation securely***

- ***Photographs, videos and images:*** Only take photographs on your mobile devices using the Spire Photography App (to be replaced our PACS Carestream photography solution at the end of 2019). Details on how to access the app will be made available when it is ready. We are aiming for it to ready by May 25th 2018. Where image storage is anonymised, consultants need to be comfortable that all risk of patient re-identification has been eliminated. Please note that the use of personal devices for image storage is likely to be a concern to the ICO and breach GMC and CQC guidance. (GMC: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/making-and-using-visual-and-audio-recordings-of-patients (2011)
  CQC guidance: http://www.cqc.org.uk/guidance-providers/gps/nigels-surgery-62-photography-making-using-visual-recordings-patients).
- **Higher Quality Images**: We have been advised that some consultants need to obtain higher quality images and therefore use personal cameras to take images (e.g. cosmetic surgeons in case of litigation) – we will review the security measures Spire would require for this and outline our requirements in the next GDPR update.
- **Dictation** solutions that email an encrypted file straight to your medical secretary and do not store recordings on the mobile device are preferred, as they are the most secure. Spire uses such a dictation solution. It is a commercial version of Winscribe. (Some consultant users were initially resistant to moving to Winscribe but now wouldn't be without it.)
- **Analogue dictaphones** with removable storage devices should be treated in the same way as paper and tapes should be wiped immediately after transcription.

C.5. ***Secure Faxing***

- Use fax machines as a last resort. Obtain a confirmation of transmission and an acknowledgement of receipt. Send faxes from and to safe locations only accessible to people with legitimate rights. Include a front sheet with a confidentiality clause. (Note: we are aware that faxes sent to/from laptops may use a different technology and we are investigating whether there this creates any additional security issues.)

C.6. Secure Telephony

- Conduct conversations in a private location where you cannot be overheard, with a person whose identity has been confirmed and has a justifiable reason to be informed regarding the SPPD. Calls should be not be recorded by the organisation or person that you are calling (many businesses automatically record all calls).
- **Voicemails** may be left for Spire patients on mobiles or landlines. The message must be restricted to who you are, who you are calling on behalf of and your contact details. (e.g. for a medical secretary: "Hello, I am calling from Mr/s xxx's office, please call could you call me back [your contact details]), or for a consultant "Hello, I am Mr/s xxx, please call could you call me back [your contact details]), or for a Spire employee "Hello, this is [x] from Spire, please could you call me back [your contact details].
- Only leave voicemails when you are confident they will only be accessed by the intended recipient and be particularly cautious with landlines.
- Do not leave messages with anyone who is not the intended recipient.
- Stop any recording of a call whilst credit card details are provided.

C.7. Other security matters

- **Whatsapp:** Do not use whatapps to transmit SPPD. NHS Digital and NICE have specifically said that they have not been able to confirm that whatapp is sufficiently secure for the transfer of patient data. We believe that they may be updating their guidance shortly but in the meantime, Spire does not consider it appropriate to counter the NHS guidance.
- Ensure any medical device or equipment that you own that stores SPPD complies with these rules.
- SPPD should not be transferred or stored outside the European Economic Area without the consent of Spire's DPO (other than data securely sent to patients or referrers), as it requires stricter controls and protection. (See Annex 3 re international transfers and C8 regarding cloud storage and email providers).
- **Destroy** SPPD securely (by secure shredding or incineration for paper or complete erasure (which may require professional assistance) in the case of electronic devices.
- Exclude SPPD from bills and invoices to the extent possible. Store payment card data in accordance with Payment Card Industry Data Standards.

C.8. Global cloud email and storage providers

Challenges with using global IT providers for cloud email and storage services

Issues arise from using providers like Gmail, iCloud and Dropbox because they are classified as your DPs. You must therefore **either obtain informed patient consent** or;

a) check that any DP will process SPPD in accordance with GDPR: the DP must provide "sufficient guarantees" of compliance; and
b) have a written contract that controls the way the DP conducts its tasks and ensures its GDPR compliance; and
c) take into consideration the fact that most global email/storage providers could be storing your data anywhere around the world: GDPR places additional restrictions on the transfer of data outside the EEA. See Annex 3 and the ICO's guidance ***https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/.;*** and
d) document the due diligence that you have undertaken on your providers; and
e) provide details of the transfers in your privacy notice.

In practice, individuals are likely to find checking the compliance of and obtaining adequate contracts from global cloud providers difficult, particularly in the early stages of GDPR as email/storage providers work their way towards compliance. ICO are understood to have recognised this issue and we have heard that they may provide some guidance in the relatively near future.

Proposed Solutions

(A) Cloud storage:

Spire does not recommend the usage of cloud data storage, unless you have been able to satisfy the provider meets the GDPR requirements above (C.8 a to c).

- As a first step, we recommend you look at services professing to be GDPR compliant. These are more likely to be paid for services aimed at the business market e.g. some consultants have advised us that the Dropbox business offering mentions on its website the provision of GDPR compliant DP contracts etc. Note that many of the free services explicitly restrict commercial usage which therefore, by definition, will not be GDPR compliant.
- ***Spire intends to offer a storage solution by making a secure drive available "SpireDrive" for consultants and their medical secretaries to use for SPPD.*** It would be hosted on Spire servers in the UK. We would also provide an appropriate DP contract. Recognising time is of the essence, we will confirm to you as soon as possible whether we can provide SpireDrive and the provisional timing. (N.B. Spire staff are only permitted to store data on SpireDrive for one month but this would be waived for consultants and medical secretaries.) In the future, the SpireDrive would become part of the consultant portal. The consultant portal is currently being rolled out across the Spire network with a target completion date of July 2019. The first phase of the portal provides consultants and medical secretaries with the ability to view patient administration details held on Spire systems and to make patient bookings. Ask at your hospital about the consultant portal or its predecessor "clinic viewer" at your hospital.

(B) Cloud email

Spire does not recommend the usage of cloud email suppliers, unless you have been able to satisfy yourself that the provider meets the GDPR requirements above (C.8 a to c).

- As a first step with cloud providers, we recommend you look at services professing to be GDPR compliant. These are more likely to be **paid for services** aimed at the business market e.g. the Dropbox business offering mentions on its website the provision of GDPR compliant DP contracts etc. Note that many of the free services explicitly restrict commercial usage which therefore, by definition, will not be GDPR compliant.
- An option for securely communicating sensitive data with your medical secretary is to use a GDPR compliant storage facility as a messaging solution (place the sensitive data on the drive and use another appropriate method to alert your medical secretary to it). Many consultants have successfully adopted such an approach.
- Several consultants have recommended **ProtonMail** which appears to be worth your consideration. ProtonMail's website advertises that for paid for services, messages will be encrypted between two ProtonMail users (e.g. between consultant and medical secretaries) and encryption can also be used with third parties (e.g. patients). Data is not stored outside the EEA and Switzerland (which was approved by the ICO at the time of writing). Upon request, their legal team will provide you with a data processing contract that they say is GDPR compliant. However, be warned, if you forget your password, it cannot be reset and you will lose access to your old emails (until and unless

you remember it). This could be an issue in the case of a claim, unless all patient related emails are also stored on the patient record.

- **Using secure networks e.g. NHSnet**; Be aware that if you send an email from a secure network e.g. Spire, it ceases to be secure the moment it hits the recipient's provider and the DC is the one responsible for security. NHSnet to NHSnet emails are secure and we have been advised that if you email from NHSnet to another provider the email will be encrypted if you type secure in square brackets in the title line "[secure]". You should verify this yourself.

Section D - Frequently Asked Questions….

D.1. Q. Will GDPR continue after BREXIT?

Yes. The Government has indicated that it intends to enact GDPR into UK law after Brexit, and a new UK Data Protection Act currently going through Parliament is expected to make specific extra provisions in UK law about certain matters under GDPR (such as health research). A number of important issues arising from these arrangements are out of the Government's direct control, being subject to the outcome of Brexit discussions with the European Union.

D.2. Am I insured for fines and data breaches?

Consultants should contact their insurer or defence organisation to establish whether or not they are covered.

Medical secretaries who are DPs should consider seeking advice regarding insurance given their new DP responsibilities (Annex 1).

This type of insurance is usually called cyber insurance but you should check that the terms of cover include compliance with GDPR requirements.

Note that insurance will cover claims (subject to the discretionary caveats) but most will only cover fines if the courts allow insurance to do so. Sometimes it is considered to be against public policy to allow insurance to cover fines. For GDPR, this will not be apparent until cases have been brought to court and judgements made, to develop a case law.

Set out below is some preliminary information that we have obtained from the main MDOs following enquiries we have made: consultants should not rely on this information and should make their own enquiries to verify this and find out specific information. Consultants should bear in mind the discretionary nature of most of the MDO schemes.

MDU and MPS

- MDU and MPS do not provide insurance, instead they offer a discretionary indemnity in respect of a consultant's legal liabilities. This means that they will determine whether they will indemnify on a case-by-case basis including for data breaches.
- Spire's view is that until cases have been brought, the discretionary nature of the indemnity means it is unclear whether they will, in practice, cover claims for data breaches.

Source: Membership – 12.04.2018
https://www.themdu.com/guidance-and-advice/guides/getting-ready-for-gdpr

https://www.medicalprotection.org/uk/about-mps/media-centre/media-gallery/mps-blogs/blogs/support-for-doctors/support-for-doctors-blog-posts/support-for-practices/2018/02/22/data-protection-is-changing

MDDUS

- The MDDUS only cover malpractice for clinical work.
- No data related claims e.g. information governance breaches or cyber security etc.

Source Membership Line – 12.04.2018
https://www.mddus.com/training-and-cpd/training-for-members/gp-risk-toolbox

Insurers
Whilst some insurers offer data protection insurance as an 'add-on', or as standard, many do not. You should speak to your broker to ascertain your current scope of cover. Spire's affinity consultant insurance, MedicaInsure, is able to offer cyber cover for certain policy holders (CFC). They can be contacted at www.medicaInsure.com

D.3. What are the contents of a privacy notice?

- A Privacy Notice must be:
  - concise, transparent, intelligible and in an easily accessible form
  - particularly clear if for children (Art 12)
- And must include the following information:
  - If data obtained from a third party, the source of the data
  - Legal bases of processing
  - Recipients of data (including international transfers and safeguards)
  - Right to rectification/erasure
  - If relying on consent, the right to withdraw it
  - Right to complain to the ICO
  - Retention period
  - Whether personal data is legally required, consequences if not supplied
  - Details of any automated decision-making

D.4. How can consultants ensure that a patient is covered by the Spire Privacy Notice?

Please also refer to B.5.

The law requires DCs to provide patients with privacy notices the first time data is collected from them. If the data is received from another source the PN should be provided within a reasonable time frame (at the latest within one month) or at first contact, if earlier.

In order to make things easier, we have specifically written the **Spire PN so that it also covers consultants and medical secretaries with respect to patients being seen at a Spire hospital**. It explains how consultants (and their medical secretaries) and Spire will use the patient's data and it covers activities directly relating to the patient's treatment including administration, general

communications between the care team and with referrers and billing. The Spire PN will be available on our website. Please read it to understand what is covered.

In order to be covered by the Spire PN, consultants and /or medical secretaries who are booking patients into Spire **must refer patients to the Spire PN** during the initial email exchange or telephone conversation AND in the first appointment letter, as appropriate. Bear in mind that existing patients will not have been advised of the PN so this should be covered with all patients when collecting data post 25 May 2018. Please note that the use of SPPD for further marketing communications to patients, or for research projects, will usually need explicit consent.

The Spire PN can be used if the patient has agreed that they will be attending a Spire facility. Refer the patient to Spire's PN "We hold your information carefully and safely in order that your privacy is protected. There is a notice on Spire's website that gives you more details." When the appointment letter is sent, it should also refer to Spire's PN. Please update relevant templates accordingly and you can use the same wording as above. If the appointment letter is sent out by Spire, our letters will contain similar wording to signpost to our PN.

Spire is investigating providing Spire MedSecs (and all patient facing Spire staff) with recordings on their telephone that the patient will hear prior to being put through. Spire will also add a reference to the Spire PN on all automated email footers and will update all template letters and eventually marketing literature with references to the Spire PN.

Spire employed medical secretaries (and other staff who first collect data from patients) must always refer to the Spire PN for any data they record for patients coming to Spire. If a Spire Medsec is making booking with another provider, it is for that provider to tell the patient about their PN or the consultant's. You should agree this process with your consultant as the DC.

If another provider asks any Spire MedSecs to refer to their privacy notice, please contact us at gdpr@spirehealthcare.com .

D.5. What should a consultant do if they employ a medical secretary?

There are lots of ways that consultants obtain medical secretarial services. Some use agencies, some use individuals who are themselves small businesses or self-employed. Some medical secretaries may even be family members. Others are directly employed by the consultant.

Whatever arrangement you have, it is important to make sure that you have adequate contractual arrangements in place with them. This is a good time to check your contracts. They may need to be updated to reflect GDPR, and to remove references to the 1998 Data Protection Act. You can use the third party GDPR clause that Spire will be providing. All contracts should also contain a confidentiality clause. Contracts protect both parties when it comes to dealing with special category data.

As a DC, you will be responsible for ensuring that you have appropriate data protection policies in place and employees are appropriately trained. Spire will be providing you with our suite of policies that we hope to have ready in mid-May. You may find these helpful when creating your own policies.

D.6. Not Used

D.7. What are Spire's policies for Data Subject Rights (DSR)?

All Data Subject Requests

- If the DSR is linked to actual or contemplated litigation, Spire Legal will provide further guidance (in line with the Management of Claims policy).
- Patient requests must be stamped with the date of receipt. Only written requests will be accepted by Spire.
- Maintain records of the request and evidence of the process used to verify both the requester's identity and the authority of a third party acting on the patient's behalf.
- Further detailed guidance will be provided in the Spire SARs policy being published by mid-May.

Patient information requests that include a medical record (SARs)

- Any request including a medical record should be submitted to the Spire Medical Records Department (MRD) no more than one business day from receipt. Spire will send the record directly to the patient. If Spire does not hold the whole single patient record (e.g. patients treated prior to the single patient record), the MRD will make enquiries with the consultant.
- If a medical record request includes extra information and the consultant believes that Spire (including a Spire MedSec) holds some of that data, the consultant should advise the MRD who will review and respond to the consultant. Otherwise it is the consultant's responsibility to respond. We may advise consultants to seek independent advice.

Patient information requests for data that do not include the medical record (SARs)

- If the request does not include the medical record, it is the consultant's responsibility to respond. Consultants should seek independent advice for any queries on this.
- If the consultant believes that Spire (including Spire MedSec) holds some of that data, the consultant should direct the patient to contact Spire's DPO via the dataprotection@spirehealthcare.com mailbox or by post.

Other data subject requests:

- For other requests addressed to the consultant that either reference Spire or the consultant thinks that they refer to data held by Spire, the consultant should direct the patient to contact Spire's DPO via the dataprotection@spirehealthcare.com mailbox or by post.

D.8. Which data may be included unencrypted or non-secure emails?

If the patient has agreed to receive standard emails (e.g. in the Spire registration form), the following information may be included:

- Patient contact details
- Patient Hospital or NHS number
- Name of treating consultant (but not speciality details)
- High-level department name such as: outpatients, main reception, diagnostics, imaging, physio
- Appointment location, time and date
- High-level description of appointment type such as; consultation, procedure, imaging (never the specific procedure)
- Cost of treatment for invoicing purposes (but not the treatment type or code)

All other information such as clinical information or financial details, should be sent encrypted (unless there is a medical emergency and following data protection guidance may compromise patient treatment in which case security measures appropriate to that situation should be taken and transparency maintained as appropriate).

D.9. How do I secure emails by encryption?

Spire and DGL are both using Egress Switch to encrypt emails; a secure email and file transfer software tool. Egress is a robust and easy-to-use tool and can be accessed via an app. It is also free for the recipient of the email to receive and reply to the email.

To purchase a copy of Egress Switch software which will allow you to use all of the services, either contact Egress on 0844 800 0172 at info@egress.com or https://www.egress.com/what-we-offer/email-and-file-encryption. The annual license is £80 per user per annum, for 1 to 4 users. Spire has negotiated a 20% discount for you, redeemable online by using the promotion code SPIRE20JP.

There are other encryption software packages available, and we do not require you to use Egress but patients will benefit if their care providers use the same tool.

D.10. I use DGL/Clan William practice manager, what do I need to do?

Clan William have recently issued contract amendment that seeks to provide a contract that complies with the DC/DP requirements of GDPR. They have also issued notification of a GDPR upgrade package that replaces the current password protection for emails (not deemed sufficiently secure under GDPR) with egress encryption, plus some other improvements.

If you have/are a Spire MedSec using a Spire provided and hosted DGL or you have a non-Spire medical secretary located at Spire who uses a Spire hosted DGL:

- DGL have issued a contract amendment which should be reviewed and signed by the consultant as DCs, if they are satisfied with the terms (this still applies to Spire hosted DGL solutions used by Spire MedSecs).
- If the MedSec has a Spire email address, they/you will be able to use the Spire egress encryption to email from DGL instead of the current non-compliant password protection.
- Spire IT are in discussions with Clan William about the purchase of their upgrade package (we will provide an update when they have provided the information we have requested).

If any external medical secretary is using a DGL hosted version:

- DGL have issued a contract amendment which should be reviewed and signed by the consultant as DCs if they are satisfied with the terms.
- We believe that DGL are offering their upgrade package for £20 p.c.m including access to egress. The consultant would be responsible for purchasing this. We believe emails are sent from within the DGL platform, so the Spire egress will not work, so it seems likely the upgrade package is essential to send any encrypted emails.

Further Reading

The BMA has now published guidance in relation to GDPR. It is specifically aimed at GPs, including those working in private practice but has relevance to other healthcare practitioners. https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/gps-as-

data-DCs

GMC Guidance on Confidentiality (including consent and disclosure) https://www.gmc-uk.org/-/media/documents/confidentiality-good-practice-in-handling-patient-information---english-0417_pdf-70080105.pdf .

Got a different question? If you would like to contact the Spire team please get in touch at: gdpr@spirehealthcare.com.

Annex 1 - DP obligations e.g. for self-employed medical secretaries

- only act on the written instructions of the DC
- do not use a sub-DP without the prior written authorisation of the DC
- co-operate with supervisory authorities (such as the ICO)
- ensure the security of processing
- keep record of processing
- notify any personal data breaches to the DC

DPs should also be aware that they may:

- be subject to investigative and corrective powers of supervisory authorities (such as the ICO)
- be subject to an administrative fine
- be subject to a penalty
- have to pay compensation

Annex 2 - *Am I a DP or a DC?*

(See also Section B.1).

Medical secretaries employed by their consultants must follow their consultant's policies in relation to processing patient data but it is your employer who is the DC and responsible for GDPR compliance activities.

Any consultant or medical secretary employed by Spire, must follow Spire's policies relating to processing patient data but it is Spire as your employer who is the DC and ultimately responsible for GDPR compliance.

Where Spire provides medical secretary services a consultant, it is a DP of patient data for which the consultant is DC (Spire's GDPR project team will provide a DP contract to consultant who use Spire employed MedSecs).

The ICO has provided helpful guidance on the difference between DCs and DPs:

https://ico.org.uk/media/for-organisations/documents/1546/data-DCs-and-data-DPs-dp-guidance.pdf

The definitions:
"**DC**" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed
"**DP**", in relation to personal data, means any person (other than an employee of the DC) who processes the data on behalf of the DC.
"**Processing**", in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including— a) organisation, adaptation or alteration of the information or data, b) retrieval, consultation or use of the information or data, c) disclosure of the information or data by transmission, dissemination or otherwise making available, or d) alignment, combination, blocking, erasure or destruction of the information or data

The guidance says that the following activities will only be undertaken by **DCs**:

- deciding if and what information to collect from an individual, the legal basis of processing and who to disclose the data to
- interpretation, the exercise of professional judgement or significant decision-making in relation to personal data (Para 10)
- processing of data by specialist service providers (SSP) in accordance with their own professional obligations (Para 45)
- an SSP determining what information to obtain and process and being answerable itself for the content (Para 27)
- deciding how long to hold data for and whether to make non-routine amendments

The guidance suggests that a **DP's** activities are limited to more technical aspects of an operation such as data storage, retrieval, transmission or erasure. DPs should only process data on the instruction of the DC. Some degree of control over how those functions are executed can rest with a DP such as deciding which IT systems to use, how to store data, security arrangements, retrieval and deletion methods. A company/individual providing services to another is not automatically a DP. It depends on the activities undertaken.

Spire believes that consultants and GPs practising at Spire are likely to be DCs. It is hard to see how a consultant can conduct their role without deciding which data to collect and exercising interpretation, professional judgement or significant decision-making in relation to creating/amending the medical record and clinic letters. Medical secretaries are very unlikely to be DCs, as they will typically follow consultant instructions in relation to patient data matters.

In addition, the majority of independent consultants who have Spire practising privileges under the Clinical Support Specialists' Handbook will be DCs, although there may be a few exceptions. For example a technician who operates medical machinery which automatically generates clinical reports and who does not write medical reports himself is likely to be a DP.

If you think that you may be a DP for Spire rather than a DC, please contact **gdpr@spirehealthcare.com**. We may need to establish a data processing contract with you.

Annex 3 - Transfers and storage of SPPD outside the EEA

Due to the complexities of complying with the following legislation, the Spire Data Rules do not permit you to transfer SPPD outside the EEA without the permission of Spire's DPO. (This does apply to sending information to patients and their referrers which can be covered by obtaining the patient's informed consent).

GDPR imposes additional restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. Transfers may be made to countries where the Commission has decided that an adequate level of protection exists. These are listed on the ICO's website. You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

The types of storage and processing that are likely to be an issue include **cloud storage providers** (e.g. Dropbox and iCloud) and **global email providers** (e.g. Gmail and Hotmail) because you do not

know where the data is going. International transcription services and overseas suppliers of clinical technology services e.g. bespoke prosthesis and heart monitors also require consideration.

Guidance is available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

You may also transfer personal data if the organisation receiving the personal data has provided adequate safeguards. There are a number of solutions listed in the guidance but your most likely options are to either gain the patients informed consent (which is likely to be impractical) or complete these three steps:

1. **Conduct due diligence**: the ICO's guidance confirms that DCs have a responsibility to check that any DP is competent to process in accordance with GDPR. The law requires that DPs provide "sufficient guarantees" in terms of its resources and expertise to implement measures to comply. The ICO's contract guidance is available at: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf
2. **Have a contract**: put in place appropriate contractual terms with the DP (See B.6)
3. **Be transparent** with the patient about what is happening to their data (e.g. cover in your PN (See B.5))