GDPR

Consultant & Medical Secretary Update No.2

March 2018

Are you ready?

A key change!

On Friday 25 May 2018, the law relating to personal data changes radically.

Why is this important to you?

You may remember from our first update, that the new law (the GDPR) requires that you must be able to demonstrate how you comply. A breach might result in a fine and it will be easier for patients to claim compensation if you do not follow the rules. The regulator, the Information Commissioner's Office (the ICO) has increased powers to fine: the maximum goes from £500k to €20m.

How does this affect your relationship with Spire?

Under GDPR, both Spire and consultants will be Data Controllers and will be responsible for protecting their patients' personal data. Where a consultant sees or treats a patient at a Spire hospital, the new law states that Spire and the consultant will be jointly responsible for protecting that patient's data and will be jointly liable for any breach of GDPR.

Healthcare data security is a key area of concern for the ICO. It is important that we are all compliant with GDPR, and can show to the world that we are compliant. Spire will be putting in place a mandatory Data Sharing Agreement and Rules setting out how Spire and consultants will act to protect Spire patient data in compliance with the new law.

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 Spire patients: broadly speaking, these are patients booked in through Spire for an appointment, making an enquiry to Spire that leads to an appointment or a record of their personal information, or who are referred to you (including by you acting in another clinical role) at Spire.

Another particular area to focus on is "data processing". An example of a data processor would be a self-employed medical secretary who provided typing, document preparation and medical record services to consultants.

GDPR Seminars

We are holding GDPR seminars for consultants and medical secretaries (both Spire employees and external). You should have received your invitation by now and we look forward to welcoming you on the day. We will provide you with a wealth of practical information about GDPR. You will also hear how Spire plans to support you in being compliant and will have the opportunity to ask questions.

We will be sending out further updates by email and making information available on our website over the coming weeks. We have published this update jointly with update No 3 that covers the practical and technical aspects of maintaining data security.

8 things to do now....

1. Register with the ICO

Under the current regulations consultants, as data controllers, are required to register with the ICO. From 25th May, this will be a "notification" requirement. Medical secretaries will not need to notify as long as they are solely data processors.

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/

2. Create your data inventory

Consultants, as data controllers, are **required** to maintain an up to date, written data inventory maintained for example, in a spreadsheet.

Spire Healthcare

- The data inventory 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. IT providers and self-employed medical secretaries
    - how the data and storage devices are secured (see update No.3).
- Spire's own data inventory will cover data stored on Spire premises and Spire equipment (both IT and clinical) including by Spire employed medical secretaries. As a joint data controller, a consultant's data inventory can reference the Spire data inventory for their Spire patients. You should record in your data inventory any other systems or locations where you hold Spire patient data. Your non-Spire patients should be covered separately.
- Ensure that you hold a written data retention policy and comply with it. Spire is adopting a 30 year retention policy for all medical records.

3. Create your record of processing

Consultants, as data controllers, are required to maintain an up to date record of processing:

- This written record must show how and why data is collected and processed (include third parties who receive patient data to process on your behalf).
- Third parties may include: self-employed medical secretaries, PMIs, GPs, LLPs, other consultants, other healthcare professionals, IT providers, email providers, transcription services, billing companies and debt collectors.
- The Spire record of processing will cover data processed by Spire employees and/or on Spire equipment for Spire patients, so a consultant's record of processing can reference the Spire record for this part of their practice. Your record should cover anything external to this and all non-Spire patients.

4. Create your privacy notice

Consultants as data controllers 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.

- Spire will have a Privacy Notice (PN) that will cover consultants and medical secretaries in relation to Spire patients' data for the purposes of their care at Spire.
- Consultants will need their own privacy notice to cover other circumstances e.g. patients who are not yet booked into a Spire system or who are going to attend another provider, or the provider has not yet been decided. In response to requests from consultants, we are working on an example PN that you may wish to adapt and use for your private practice. This is expected to be available in April.
- External medical secretaries who book patients into Spire will be asked to include a standard reference to the Spire PN in the appointment letter as well as the consultant PN. Wording will be provided.

5. Review and update your third party contracts

Any data stored or processed for you by a third party **must** be covered by a contract that controls the way they conduct their tasks and ensures their GDPR compliance.

- See point 3 for examples of third parties.
- Spire's Data Sharing Agreement will cover you for processing and storage where this is done by Spire or Spire employed medical secretaries.
- If you employ a medical secretary, you should ensure their employment terms comply with GDPR and protect you (see FAQ in Update No. 3).
- If you use a third party medical secretary (who you do not employ) you should have a services contract in place with them and this must include a GDPR-compliant data protection clause.
- Spire will be providing a model GDPR compliance clause as an example of the sort of provisions one would expect in an agreement to ensure GDPR compliance.

6. Where you are relying on patient consent, ensure that it is lawful

Your PN should set out the basis on which you process data. The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- **Consent**: the patient has given consent for you to process their personal data. Consent must be a clear, informed, recent, specific opt-in

- **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
- **Legal obligation**: the processing is necessary for you to comply with the law
- **Vital interests**: the processing is necessary to protect someone's life
- **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
- **Legitimate interests**: the processing is necessary for your 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

- Providing direct care and the holding of medical records should not require specific patient consent.
- Ensure that patient consent has been obtained to transfer their data as part of an onward referral process. Data being transferred to referrers and GPs is covered in the Spire Privacy Notice (see point 4 above).
- Using patient data for any other reason such as marketing, promotion (such as before and after photos), outcome data or follow-up requests from insurers is likely to need GDPR compliant consent. 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.
- Research is a special category – we will cover this in future updates as well as providing information to medical registries.

See: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

7. Ensure you are storing and processing data securely

See our Update No3 - published jointly with this one. Spire's Data Sharing Rules will be based on these.

8. Create your compliance plan

- Research your obligations: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- Set out how you will comply with your GDPR obligations to keep patient, employee or other personal data safe.
- Include a map showing how you use data and who you share it with.
- Have written data protection policies and procedures in place.
- Seek legal advice if you are unclear on your obligations.
- Identify gaps in compliance and how you will rectify them.
- Write your plan down – GDPR requires actively demonstrated compliance and if you have a breach the ICO may ask to see it.
- Keep your plan up to date.

Next steps

- Spire will be providing a further update in mid-April, prior to the GDPR seminars. This will include the Data Sharing Agreement and The Data Rules that Spire will require consultants practicing at Spire hospitals and their medical secretaries to abide by, when managing Spire patient data, in order to ensure GDPR compliance. We will also cover further items such as patient rights to access data, children and breach reporting.
- Spire plans to provide you with example documents to help consultants meet their GDPR obligations. These will require tailoring by the consultant as each consultant's practice will be different. They will not be a substitute for consultants taking their own legal advice where required. The documents will be:
  - example consultant Privacy Notice
  - blank data inventory and record of processing
  - model GDPR compliance clause for third party contracts (including medical secretaries)
  - wording for medical secretaries to put in appointment confirmation letters for Spire patients relating to the Spire PN.

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