GROUP INFORMATICS

DATA PROTECTION LEGISLATION

FREQUENTLY ASKED QUESTIONS (FAQ)

What is happening with regard to Data Protection?

New European arrangements are coming in to force on 25th May 2018. This is known as GDPR (General Data Protection Regulation).

The current UK Data Protection Act (1998) has been repealed and a new Data Protection Bill received Royal Assent on 23rd May 2018. The new Act ensures that the data protection standards set out in the GDPR, when applied in the UK, reflect the requirements of the UK. It will establish continuity in the UK post Brexit and introduce legislation where GDPR allows flexibility, cover legislation on law enforcement and national security and make provision for the Information Commissioner.

The Data Protection Act (2018) has replaced the 1998 Act as the primary piece of data protection legislation in the UK.

I've read in the media that the new law means that consent is needed to use personal data; do I have to ask every patient I see for their consent?

No, consent is not appropriate for direct care purposes and would be misleading and inherently unfair if used.

Consent is only one of six available lawful bases for processing.

The Trust, as a public body continues to have a lawful basis for processing personal data to deliver its services to patients and staff. For those that are interested, for most of its services the lawful basis is GDPR Article 6 (1) (e), which is a 'public task' basis.

I've heard reference to 'special category data'; what is this?

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. It includes information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;

- sex life; or
- sexual orientation

In order to process special category data, one of ten specific conditions needs to be met. The Trust will mostly use two specific conditions, that being processing for health care and processing for safeguarding. For those interested, these are GDPR Article 9 (2) (h) and Article 9 (2) (b) respectively.

There may be occasions when one of the other specific conditions may be met. For further advice please contact Group Informatics, Information Governance team.

Will the new law affect how I do my job?

The Trust continues to have a lawful basis for processing data to deliver its services to patients and staff. However there is a greater requirement for more transparency and accountability, so you need to ensure Trust Information Governance (IG) policies, Codes of Practice and NHS Caldicott principles are always followed.

Always ensure that personal data is accurate; for example check patient name, date of birth, address, GP, Next of Kin as a minimum at every point of contact.

The new legislation puts greater emphasis on technical and organisational measures being used to protect the security and confidentiality of personal data.

You should all have your own logon credentials (username and password) for the systems you are authorised to access. Do not share your logon credentials with anyone. If you have a generic logon to a PC, then you must treat this in the same way as your own personal logon credentials. You must not disclose these credentials to anyone else, just because it is a generic logon

Be security conscious:

- Do lock your PC if left idle.
- Don’t provide your username to something you are not sure about.
- Do not ever provide your password.

Do keep all personal identifiable data safe and secure. This applies to data held electronically and in paper form. Please see the Handling Personal Identifiable Data Code of Practice for further information.

Will I have to ask patients for their consent before I can use their health records for direct care?

No. With regard to processing patient data for direct health care (including administrative purposes), the Trust does not need consent as it has another lawful basis and condition under the new legislation which is that of a public task – the Trust is processing healthcare data in order to carry out its function, which is that of health care.

Clinical consent for an operation or other treatment is completely separate as it is not the same as consent for processing data. You must continue with clinical consent in the same way as you do now. The clinical consent decision will still need to be documented (processed) in the health record.

What should I do if I'm asked by a patient about their data?

The Trust has a privacy notice which informs patients of how the Trust uses their data, the lawful basis and condition for doing so and their rights under the data protection legislation. Please ensure that these leaflets are available within your own areas for patients to pick up.

If you do not have any, please contact Information.governance@mft.nhs.uk

What should I do if a patient wants to see their data?

As before, patients are able to request to see their data. This does not mean that patients can view their records at any time. The Trust process for accessing personal records must be followed. This applies to requests from staff as well as patients.

The new legislation introduces new changes including the removal of the fee; the request to see their data no longer needs to be in writing, a verbal request is sufficient and the Trust now has to respond within one calendar month.

If a request for health records is received then it must be forwarded to the Subject Access Request (SAR) Team (formerly medico-legal team) promptly.

If the request is made verbally then, where possible, please confirm the identity of the requestor at the time of request and make sure that this is documented and forwarded to the SAR team immediately. Forms for recording this information will be available on the Intranet soon.

Please support the SAR team by providing case notes and other information as soon as there is a request so that the timescales can be met.

If you receive a staff request for information about their personal data, please discuss this immediately with your line manager, Human Resources representative or Group Informatics, Information Governance team.

Are there other individual rights under the new legislation?

Individuals have a number of rights under the new legislation; these include the right:

- of access
- to rectification

- to erasure*
- to restrict processing, where applicable
- to data portability*
- to object
- not to be subject to automated decision making including profiling

*The right to erasure and the right to data portability are not applicable when processing on the basis of a public task.

If a patient requests a right under the Data Protection legislation, what should I do?

In the same way as requesting to see their data, the Trust must respond to the other individual requests within one calendar month.

The Group Informatics, Information Governance (IG) team will provide advice on how to manage these requests. If you receive such a request please contact the IG team on: Information.govenance@mft.nhs.uk

Can patients still receive text reminders, phone alerts about their appointments?

Yes, this is part of the administrative service that we offer.

What about emailing patients?

Newsletters and other patient information can be emailed to them. However before doing this it is good practice to check that the patient is aware of the risks that this method of communication may have (such as for example, shared personal email account) and record their acknowledgement of these risks in their health record.

It is recommended that emails to patients that contain details of their healthcare are sent using email encryption. This is easy to use – you just need to put [encrypt] in the 'subject' box and then compose and send the email as normal.

Please remember that the new law puts greater emphasis on the provision of technical measures so do ensure that, when emailing patients, great care is taken when inputting the email address in the 'to' box.

Further guidance can be found in the Handling Person Identifiable Information Code of Practice and the Code of Practice for IT, Internet and Email Use.

You cannot send any marketing material by text or email unless the individual has signed up to allow this.

I've been told that some private practices are stopping current processes such as emailing patients, not allowing the movement of files. Is this prohibited by the new law?

The new legislation doesn't specifically mandate restrictions such as not emailing patients or restricting the movement of patient files. However the new legislation does put greater emphasis on the provision of technical measures to ensure the security, confidentiality, integrity and availability of personal data.

Organisations must have technical or organisational measures in place so that processing of personal data is done in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The Trust has a number of policies and documents such as the Code of Practice for the use of IT, Internet and Email and Handling Personal Identifiable Information Code of Practice, both of which outline the technical and organisational measures that staff must follow when processing personal data, be it through the use of IT, physical transportation or verbally.

Some smaller organisations such as private practices may consider that their current processes are not robust enough to provide the appropriate technical measures and have therefore introduced restrictions.

It is important that you are aware of the technical and organisational measures that you must follow when using personal data.

Can I give patient information to the police?

The police still do not have an automatic right to patient or staff records. A standard operating process for handling police requests will be available soon on the Intranet. If the request is very sensitive or complex then the decision to disclose should be taken in consultation with the Information Governance team who will liaise with the Trust Caldicott Guardian as appropriate.

How does the Common Law Duty of Confidentiality fit in?

Most patients understand and expect that relevant information must be shared to the appropriate health and care professionals for the provision of their direct care. This is explained in the Trust's privacy notice.

NHS Caldicott principle 7 states "the duty to share is as important as the duty to protect patient confidentiality".

Disclosure of patient data is essential for provision of safe and effective direct health care and relevant information about a patient should continue to be shared between health and care professionals in support of their direct healthcare.

So I can continue to disclose relevant, justified, proportionate data for direct care to another health and care professional within and outside of the Trust?

Yes, as long as it is for direct patient care, NHS Caldicott principles are followed and robust technical security measures such as encrypted emails are used then patient information can be shared.

I want to start sharing bulk patient data with another organisation on a regular basis, can I just do this?

Before regularly sharing patient data with another organisation, a Data Protection Impact Assessment (DPIA) needs to be completed and submitted to the Informatics Governance team for approval. The IG team will assess that there is a lawful basis for processing the data, that the sharing is proportionate, to be shared securely and confidentially and within NHS Caldicott Principles.

What about using patient data for research?

As part of our public task we undertake vital health and care research. As a public body, our lawful basis for processing data for research purposes is a task in the public interest. Before any research is commenced, the researchers must present their case before an ethics committee to check that their research is appropriate and worthwhile.

At the start of the process for undertaking any research a Data Protection Impact Assessment is completed and submitted to the Information Governance (IG) team who will assess that there is a lawful basis for processing the data, that the sharing is proportionate, to be shared securely and confidentially and within NHS Caldicott Principles.

Further guidance on the use of identifiable data, and how it can be used for research under the new legislation, will be communicated as soon as it is available.

What if I want to share anonymised data?

A shortened DPIA for anonymised data needs to be completed and submitted to the IG team. This is to provide assurance that data is truly anonymised and cannot become identifiable.

Where can I find a DPIA template?

The DPIA templates are being re-drafted and will be placed on the Intranet in the next few weeks. Until then, please contact the IG team on information.governance@mft.nhs.uk

The new legislation mandates that a DPIA must be completed for certain listed types of processing or any other processing that is likely to result in a high risk to individual's interests.

The IG team will be scheduling fortnightly Data Protection Privacy Panel to review and approve submitted DPIAs. A timetable for these panels will be posted on the Intranet.

If I want to send data overseas, do I have to do anything?

The new legislation imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

Please contact the Information Governance team if you want to send patient data overseas.

How long do I need to keep personal information?

The Trust follows NHS Digital Records Management Code of Practice for Health and Social Care 2016 which can be found at:
https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

How do I destroy personal data?

All wards and departments have been provided with at least one grey locked console which must be used for disposal of any paper containing confidential and non-confidential information.

Please contact the informatics Service desk for disposal of hardware including PCs, printers, faxes, portable hard drives etc.

What happens if there is a breach of personal data?

The Trust must report certain types of personal data breach to the Information Commissioner's Office (ICO). Additionally, the legislation states that a record of any personal data breaches must be kept, regardless of whether they need to be reported or not.

The Trust must be able to detect, investigate, report (both internally and externally) and document any breaches.

If there is a breach of personal data then this must continue to be logged without delay on the Trust Incident reporting system as you do currently. If you are unsure of the severity level please contact Information Governance team.

As before, Group Informatics, Information Governance team will decide on whether the breach needs to be escalated and reported to the ICO.

Have all the Information Governance policies and Codes of Practice been updated?

These are being updated to reflect the new legislation, however as the Data Protection Bill is still progressing through Parliament, all changes have not been finalised.

The technical and organisation measures currently in place will remain and you must ensure that you follow existing policies and procedures until the new documentation is uploaded on to the Trust Intranet.

If you have any further queries regarding Data Protection and / or Information Governance then please contact Group Informatics, Information Governance team at: Information.governance@mft.nhs.uk