Data Protection Impact Assessment (DPIA)
Phyllis Tuckwell Hospice Care – GP records EMIS Project

Need for a DPIA

The Phyllis Tuckwell Hospice Care (PTHC) data sharing project requires a DPIA.

This project fulfils several criteria that warrant a DPIA:

- *Processing special category data* – health & social care data
- *Scale* – the data extraction potentially involves every patient of the GP practice (unless they have specifically opted out)
- *Children* – the GP records of children (from birth) are *potentially viewable*
- *Vulnerable adults* – the GP records of vulnerable adults are *potentially viewable*
- There is access to the *full* GP record

The nature of the processing

This project aims to facilitate bidirectional sharing of information of patient health records between the practice and PTHC.

PTHC has performed a detailed and very helpful PIA which should be referred to for further detail.

Clinicians and appropriately authorised administrative staff at PHTC will, with the consent of the referred patient, be able to access the *full GP record* of that patient. Equally, the practice will be able to see the full PTHC record of the patient (within EMIS Web).

The data shared consists of the medical records as held by each organisation. Each organisation remains the data controller for their records – no data is transferred from one controller to another, and no data processors are involved.

Access to the GP records is limited to authorised PTHC staff *involved in clinical care.*

Scope of Processing

see Schedule A of the PTHC PIA

PTHC will have access to the full GP record of a referred patient, including medication, consultations, allergies, test result and documents.

The information is viewed in real-time, i.e. *streamed:* no data is uploaded or transferred from one data controller to another.

The practice remains the data controller for the GP record, and PTHC remains the data controller for the PTHC record.

Context

The individuals concerned are patients registered with the GP surgery and of need of referral to PTHC for *direct medical care.*

Individuals have the right to "opt-out", i.e. object, by requesting to the GP practice that they do not wish for their GP record to be viewable by PHTC in this way. They can also request that individual items within their GP record are marked as "confidential", that is not viewable by organisations outside of the GP practice.

Individuals include children and vulnerable adults.

When a patient is referred to PTHC, relevant clinical information is provided within the referral process. Access to the GP record is supplementary to this and may save time for both data controllers as additional information (such as hospital letters and scan results) are often subsequently requested. In time, it may be that a formal detailed referral becomes unnecessary.

However, patients do not currently expect their *entire GP record* to be viewable by an organisation such as PTHC.

We have experience of data sharing in this way – the MIG is a similar scheme that allows real-time data streaming of GP records to FPH A&E and NHUC GP OOH, although the data available is less comprehensive that the full GP record.

Purposes

The sole purpose of this project is to facilitate *direct medical care.*

Such processing has but one aim – to make available information from the GP record to healthcare professionals outside of the GP surgery, where direct care is being provided by that professional.

The aims (benefits) of this project are:

- To share Health Records ensuring information is available to inform clinical decision making e.g. patients care and treatment at the point of need
- Quicker and more efficient referral process

- Faster documentation therefore more time available for patient contact in part by more automated documentation and better design
- More efficient patient journey
- A more paper light service
- More accurate reporting
- Fewer errors in patient bookings
- Overall reduced opportunities for human error

Consultation process

The practice does not consider it necessary to run a formal consultation process. Referrals to this organisation are well established and long-running, and the sole purpose of such processing is to facilitate and improve direct medical care. Detailed information, including much of what would be available to PTHC via this project, is already provided to PTHC during the referral process, and subsequently as required.

It would be difficult to identify a cohort of patients who *might* need the services of PTHC in the future – *all* patients are at risk of cancer and other terminal diseases.

Data protection compliance (necessity and proportionality)

Common Law (CLoC)

Since the disclosure of data to PTHC is purely for direct medical care purposes, it could be argued that *implied* consent could be relied upon to satisfy the CLoC.

However, whilst that is true for the information provided to PTHC within the current referral process, it might come as a surprise to patients that, unbeknown to them, their full GP record was being made available in this way.

PTHC state that they will seek *explicit consent* from patients (unless impracticable, such as an unconscious or uncommunicative patient, where access to the record would be in the public interest to safeguard the welfare of the patient). This would clearly satisfy the CLoC, particularly if practices also sought the explicit consent of patients to permit the sharing of their GP record in this way at the time of referral.

Caldicott Principles

1. Justify the purpose(s)

The purpose for such data processing has been detailed and justified.

2. Don't use personal confidential data unless it is absolutely necessary

For direct medical care purposes, it is essential to use personal confidential data.

3. Use the minimum necessary personal confidential data

Access to the full records of each organisation will be available.
See later under risks and mitigating factors.

4. Access to personal confidential data should be on a strict need-to-know basis

PTHC have safeguards in place to ensure that only those authorised to view GP records within their organisation can do so.

5. Everyone with access to personal confidential data should be aware of their responsibilities

PTHC ensure that this is the case.

6. Comply with the law

This project is lawful (see Article 5 GDPR below)

7. The duty to share information can be as important as the duty to protect patient confidentiality

The sharing of detailed information from the GP record in such circumstances is important.

Article 5 GDPR – the data protection principles

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals (lawful purpose)

for PTHC – see Schedule A of their PIA

The practice will rely upon the very same lawful bases for such processing, namely Article 6(1)(e) – Official Authority and Article 9(2)(h) – Provision of Health.

Both organisations must provide comprehensive fair processing information, in line with the GDPR, and ensure data subject rights such the right to object, the right to access and the right to rectification.

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)

The sole purpose of such processing is to enhance the direct medical care of referred patients. There are no other purposes (such as secondary uses).

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)

Access to the full records of each organisation will be available.
See later under risks and mitigating factors.

d) accurate and, where necessary, kept up to date (accuracy)

Both PTHC and the practice already have obligations to maintain the accuracy of their respective records.

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation)

No data is transferred from one controller to another, and each controller already has obligations to ensure lawful data retention policies for their respective records.

f) processed in a manner that ensures appropriate security of the personal data (confidentiality)

The ability to view each other's records in this way takes place in a secure cloud-based, encrypted environment, hosted by EMIS Health, and via secure communication channels. Only those authorised (by each organisation) to view such records can do so.

No data is transferred anywhere, including outside of the EEA.

Risks

OHG has identified a number of *potential* risks:

The use of minimum necessary confidential data

The third Caldicott principle and Article 5(1)(c) both refer to the use of the minimum data that would serve the purpose of the processing.

It might be argued that access to the entire GP record would permit disclosure of information that is not necessary for PTHC to be aware of. However, it would be very difficult to know, in advance, what might and might not be relevant within a GP record, given the wide-ranging services that PHTC provides to patients, both in terms of medical treatments and psychological support (such as counselling). The withholding of clinical data in this way could result in sub-maximal therapy for patients. End of life care can present management issues that encompass symptoms and signs throughout the human body, and it could be argued that it is essential to know the full medical history of the patient to avoid misdiagnosis and inappropriate, or even harmful, management. The care that PTHC provides is holistic and relates to every system in the body – not unlike GP care.

There is potential access to the GP record of every patient, even if there was no legitimate relationship with PTHC

In theory, with very basic demographic data, PTHC could access the GP record of any of the practice's patients (unless they had opted-out). This would include children, which PTHC does not (generally) provide services to.

Management of opt-outs

The mechanism by which patients can object to (or opt-out of) permitting access to the GP record by PTHC is not clear. It is likely that dissenting from EMIS Web data sharing (the 93C1 read code) will achieve this, but how other opt-outs, such as the SCR (9Ndo) and Hampshire Health Record/Risk Stratification (9Nd1) might also result in the inability of PTHC to view the GP record.

The EMIS Web data sharing opt-out is the mechanism by which patients can object to the MIG – the data sharing project that allows FPH A&E and NHUC GP OOH access to GP records. Some patients (at this practice, approximately 155) have expressed such an objection and it may be that their GP record would be unable to be viewed by PHTC, should a referral take place.

Those patients are not currently aware of this "extension" to their opt-out, and indeed they might not want PTHC to be denied such access.

Very many more (in excess of 2000 patients) at this practice have expressed an objection to the SCR or the HHR or (historically) risk stratification for case finding.

Historic patients

Patients referred to PHTC prior to the commencement of processing will neither have been informed that their GP record would/could be accessed in this way, or of their right to opt-out. They might have their record accessed by PTHC in the absence of their explicit consent, under a belief or assumption that access was permissible in the absence of an objection.

Measures to reduce or eliminate risks

The use of minimum necessary confidential data

Ensure extensive fair processing information is easily available to patients.

This would include the fact that the *entire* GP record is made available to PTHC, but that patients can request that specific entries are not visible to PTHC.

Ensure patients understand their right to object – to opt-out.

EMIS Web does permit "*confidentiality policies*" – at either the patient's request, or the GP's decision, individual entries within the GP record can

be "hidden" from access/viewing by an organisation outside of the practice (such as PTHC).

Risk status: Low risk

There is potential access to the GP record of every patient, even if there was no legitimate relationship with PTHC

Access to the GP record within PTHC is strictly controlled (and vice versa).

A detailed and comprehensive data sharing agreement would be in place between PTHC and the practice.

Both organisations have codes of practice and confidentiality agreements within employment contracts.

Both organisations can (and should) conduct regular access audits. This is easily done within EMIS Web.

Both organisations should remind its employees of the serious consequences of in appropriate access, including disciplinary action.

Risk status: Low risk

Management of opt-outs

Clarity will be needed on exactly how patients can object and how the individual existing opt-outs interact with the PTHC project.

Comprehensive fair processing information must be then made available to patients to ensure that they understand what they have opted out from.

A sole and specific opt-out code from the PTHC project should ideally be identified (if possible), one which will not affect any other data sharing project (such as the MIG). However, this is rarely possible in the field of data sharing.

If, as might be the case at Oakley Health Group, there are relatively few patients with an existing opt-out that would impact upon the PTHC project, those patients could/should be written to on an individual basis to explain the "extension" to their opt-out and whether they wish to amend their objections (if possible) accordingly.

Risk status: Medium risk

Historic patients

There will need to be clarity about how the records of patients previously referred to PTHC, or already under their care will, or will not, be accessed.

Such patients will need to have their explicit consent obtained by PTHC *before* their GP record is accessed, either in advance or opportunistically.

This may require some sort of "alert" on PTHC's clinical record to ensure that the explicit consent of the patient is obtained before their GP record is first accessed.

Alternatively, PTHC could mandate it so that only patients referred to their service on or after a certain date would have their GP record accessed in this way.

This may require some sort of "alert" on PTHC's clinical record to ensure that the GP record is not inadvertently accessed.

Risk status: Medium risk

Conclusion

Permitting access to the GP record by PTHC, for the sharing of sensitive data *for direct care purposes only,* is lawful and compliant with common law, the Caldicott Principles, and the data protection principles as listed in Article 5 of the GDPR.

The practice retains absolute *data controllership* of the processed data.

OHG must provide extensive fair processing information to our patients about this potential use of their health data and of their right to object ("opt out"), and any other such rights under GDPR. Patients should also understand that they can request a confidentiality policy be applied to any item within their GP record.

There are risks associated with such processing, but those risks can be mitigated successfully. Some of these mitigations will be the practice's responsibility, others that of PTHC.

Accordingly, the processing would **not** result in a high risk to the rights and freedoms of natural persons and there would be no need to consult the supervisory authority prior to such processing.

Sign Off

This DPIA will:

- Be circulated to all GP partners at OHG to decide whether to proceed with such processing
- In the event of agreement to proceed with this project, be published and available to patients, linked to within our privacy notice for this processing
- Be disclosable under FOI

Dr Neil Bhatia

GP, IG/FOI/Records Access lead, Caldicott Guardian, DPO
Oakley Health Group

24.07.18

Addendum:

The GP partners voted in a majority to proceed with processing in this way. There were no objections.

The Hospice was informed of the decision on 29th July.

Dr Neil Bhatia's vote was not recorded and did not count (as he is the DPO and was responsible for the DPIA).