From: FOIA s.40(2)
To: Maddy Griffiths
Subject: RE: Clinical trials advice - Query about terminologies
Date: 12 March 2020 09:44:36
Attachments: image001.png

External: This email originated outside the ICO.

Hi Maddy – sorry I was in a meeting earlier

The person who is responsible for the Clinical Trial is the 'Sponsor'

It would be the Health Trust/Health Board that is responsible for the EHRs

Best wishes

FOIA s.40(2)
[redacted]
Expert Inspector, GCP
FOIA s.40(2) [redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

From: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Sent: 12 March 2020 09:25
To: FOIA s.40(2) [redacted]
Subject: Clinical trials advice - Query about terminologies
Importance: High

Hi FOIA s.40(2) [redacted]

The advice is nearly complete

I've made a couple of 'phonecalls to you this morning – I just wanted to check about terminologies in the health sector.

Is there a specific term used to describe 'the data Controller holding the EHRs'?
Hospital? Health Trust?

Is there a specific term for 'the organisation commissioning the clinical trial?'

I want to make the advice as clear as possible – sector-appropriate terminology will be a benefit.

Best wishes,

Maddy.

Signature2

Maddy Griffiths
Senior Policy Officer – Regulators' Business Innovation Privacy Hub
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6303 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For information about what we do with personal data see our privacy notice

---

From: FOIA s.40(2)
Sent: 02 March 2020 07:39
To: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Cc: Helena Wallace <Helena.Wallace@ico.org.uk>
Subject: RE: Access to Electronic Patient Records - MHRA Position Statement

External: This email originated outside the ICO.
Hi Maddy – yes this would be helpful as we want the advice to cover all of the UK. I wasn't aware of any specific differences in relation to the issue we are talking about.
Kind regards

FOIA s.40(2)
Expert Inspector, GCP
FOIA s.40(2)
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

From: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Sent: 28 February 2020 16:15

To: FOIA s.40(2) [redacted]
Cc: Helena Wallace <Helena.Wallace@ico.org.uk>
Subject: RE: Access to Electronic Patient Records - MHRA Position Statement

Dear FOIA s.40(2) [redacted]

I have prepared the draft advice for you regarding clinical trial data (bar a few closing comments).

My office would like a little time to look over the advice prior to release to MHRA – which I should have anticipated and allowed for in my timescales.
Whilst I do not wish to keep you waiting it is very important to me that any advice I send is fully approved by my office, particularly as it must be suitable for the many organisations who would like to benefit from the proposed joint advice from the ICO and MHRA.

An area I have not covered in my draft advice is any regional differences for the devolved administrations. Would this be helpful? I'm happy to consider it whilst I await feedback from my office.

My sincere apologies for this delay.

All my best wishes,

Maddy.

Signature2

Maddy Griffiths
Senior Policy Officer – Regulators' Business Innovation Privacy Hub
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6303 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For information about what we do with personal data see our privacy notice

---

From: FOIA s.40(2) [redacted]
Sent: 24 February 2020 10:18
To: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Subject: RE: Access to Electronic Patient Records - MHRA Position Statement

External: This email originated outside the ICO.

Yes that's great, thanks Maddy
Best wishes

FOIA s.40(2)
[redacted]
Expert Inspector, GCP
FOIA s.40(2)
[redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

From: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Sent: 24 February 2020 10:08
To: FOIA s.40(2) [redacted]
Subject: RE: Access to Electronic Patient Records - MHRA Position Statement

Hi FOIA s.40(2) [redacted]

I'm hoping to have a draft sent out to you by Friday – hope this helps?

Will be in touch.

Best wishes,

Maddy

From: FOIA s.40(2) [redacted]
Sent: 21 February 2020 16:14
To: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Subject: RE: Access to Electronic Patient Records - MHRA Position Statement

External: This email originated outside the ICO.
Hi Maddy – I haven't heard from you in a while, just checking to see where we are with our joint statement – is there anything I can do?
Have a good weekend

FOIA s.40(2)
[redacted]
Expert Inspector, GCP
FOIA s.40(2)
[redacted]
I,E&S/Library

National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

From: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Sent: 14 January 2020 14:46
To: FOIA s.40(2) [redacted]
Subject: RE: Access to Electronic Patient Records - MHRA Position Statement

Hi FOIA s.40(2) [redacted]

Tuesday at 2:30pm is perfect

Best wishes,

Maddy

From: FOIA s.40(2) [redacted]
Sent: 14 January 2020 14:23
To: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Subject: RE: Access to Electronic Patient Records - MHRA Position Statement

External: This email originated outside the ICO.
Tuesday at 2.30?
You can call my mobile or the landline number
Look forward to speaking to you soon

FOIA s.40(2) [redacted]
Expert Inspector, GCP
FOIA s.40(2) [redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

Stay connected: mhra.gov.uk/stayconnected
MHRA is a centre of the Medicines and Healthcare Products Regulatory Agency

---

From: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Sent: 14 January 2020 14:18
To: FOIA s.40(2) [redacted]
Subject: RE: Access to Electronic Patient Records - MHRA Position Statement

Hi FOIA s.40(2) [redacted]

Tuesday after 2pm would be good, or Thursday before 12 noon, or Friday before 12 noon.

Best wishes,

Maddy

From: FOIA s.40(2) [redacted]
Sent: 14 January 2020 14:09
To: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Subject: RE: Access to Electronic Patient Records - MHRA Position Statement

External: This email originated outside the ICO.
Hi Maddy
I'm in a meeting in London all morning on Friday. Next week I am free all day Tuesday, or weds afternoon – and Thursday and Friday are fairly clear, so next week is much better if that suits you?
Best wishes

FOIA s.40(2) [redacted]
Expert Inspector, GCP
FOIA s.40(2) [redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

Registration is now open for the MHRA Good Clinical Practice Symposium.
This Symposium is in partnership with the US Food and Drug Administration (FDA).
Thursday 13 – Friday 14 February 2020
Engage with us *#MHRAGCP20*

Stay connected: mhra.gov.uk/stayconnected
MHRA is a centre of the Medicines and Healthcare Products Regulatory Agency

---

From: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>

Sent: 14 January 2020 14:01
To: FOIA s.40(2) [redacted]
Subject: RE: Access to Electronic Patient Records - MHRA Position Statement

Hi FOIA s.40(2) [redacted]

Happy New Year!

Yes – how would Friday morning (ie. before 1pm) suit?

Best wishes,

Maddy

From: FOIA s.40(2) [redacted]
Sent: 10 January 2020 15:23
To: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Subject: RE: Access to Electronic Patient Records - MHRA Position Statement

External: This email originated outside the ICO.
Hi Maddy
Happy New Year!
FOIA s.40(2) [redacted] shall we try to catch up again on this issue soon?
Kind regards

FOIA s.40(2) [redacted]
Expert Inspector, GCP
FOIA s.40(2) [redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

From: FOIA s.40(2) [redacted]
Sent: 03 December 2019 09:42
To: Madelaine.Griffiths@ico.org.uk
Subject: RE: Access to Electronic Patient Records - MHRA Position Statement

Hi Maddy – it was good to talk to you a few weeks ago. I'm now back from my holiday and wondered if you had progressed this any further and whether we can find time for a catch up?
Best wishes

FOIA s.40(2)
[redacted]
Expert Inspector, GCP
FOIA s.40(2)
[redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

Registration is now open for the MHRA Good Clinical Practice Symposium.
This Symposium is in partnership with the US Food and Drug Administration (FDA).
Thursday 13 – Friday 14 February 2020
Engage with us *#MHRAGCP20*

Stay connected: mhra.gov.uk/stayconnected
MHRA is a centre of the Medicines and Healthcare Products Regulatory Agency

---

From: FOIA s.40(2)
Sent: 30 October 2019 13:02
To: Madelaine.Griffiths@ico.org.uk
Subject: Access to Electronic Patient Records - MHRA Position Statement

Dear Maddy

We have dealt previously (back in 2014) with this query and MHRA and ICO came to an agreement about how this could be addressed. We would like to publish a joint position statement on this, as it still seems to still be a problem in clinical research.

Patents when they consent to take part in a clinical trial consent to their records being reviewed by monitors from the sponsor. Obviously the EHRs contain information on all patients in the hospital/Trust, so monitors should not have access to those records outside their clinical trial – however most systems are not designed with this functionality to restrict access – so this often results in sites printing out records for monitors to review, rather than giving them direct access and trusting them to only look at their trial patients.

ICO advice on how to manage this was that an agreement between the Trust and the monitor would be sufficient, if they were provided with training to ensure that those given access to the data understood the boundaries and patients' rights in terms of data protection. If their actions went beyond that, that they would be guilty of a breach of the data protection act. The system should have an audit trial, so that it can be demonstrated (if needed) that the monitor did not look at records of patients outside the clinical trial that they had consent to review.

Although we pass on this advice, Trusts are still insisting on printing out EHRs. Printing out – as well as being time consuming – has produced some issues, such as not all the information being

printed – so medical histories have been incomplete, and important information such as drug reactions have been missing. We have seen gaps in dates – so reports are printed from one date to another – we've seen gaps in the print outs which has meant weeks of missing data, potentially missed safety events.

So, we would like to create a joint position statement with the ICO to address this, therefore I would really welcome a discussion around this with you

I look forward to hearing from you soon
Kind regards

FOIA s.40(2)
[redacted]
Expert Inspector, GCP
FOIA s.40(2) [redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

From:	Maddy Griffiths
To:	FOIA s.40(2)
Cc:	Helena Wallace
Subject:	Advice from the ICO Innovation Hub regarding access to EHRs
Date:	30 March 2020 23:02:00
Attachments:	image001.png 20200330 ICO Innovation Hub advice to MHRA regarding access to EHRs .pdf Innovation Hub business terms and conditions.pdf

Dear FOIA s.40(2)

Please find attached the advice from the ICO Innovation Hub regarding access to EHRs for clinical trials.
This advice has been written to assist and inform MHRA in the production of the new advice regarding EHRs, in accordance with the ICO Innovation Hub terms and conditions, which I also attach.

When the advice written by MHRA is finalised, the ICO Innovation Hub would appreciate being sent a copy for approval prior to any publication on the MHRA website or dissemination by other means, to ensure that the advice as written here is clear and is accurately represented in the final document.

I have incorporated input from the ICO regions in producing this advice to reflect the differences in terminologies used in Northern Ireland, Scotland and Wales.

I hope you will find the attached advice useful. If any points are unclear please do not hesitate to contact me.

All my best wishes,

Maddy Griffiths.

Signature2

Maddy Griffiths
Senior Policy Officer – Regulators' Business Innovation Privacy Hub
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6303 ico.org.uk
twitter.com/iconews

Regulators' Business Innovation Privacy Hub

Advice Provision Form

This advice is given in accordance with the terms and conditions supplied with your confirmation letter

Nature of advice sought	Information received
Include the project/work plan to which the advice relates MHRA would like advice from the ICO Innovation Hub regarding clinical trial data - specifically, facilitating access to EHRs and the handling of patient data. This advice from the ICO will inform new advice from MHRA aimed at the Health Trusts and Health Boards who hold EHRs. MHRA may put their finalised advice on their website.	*Include links/references to contact notes as relevant* Advice request from MHRA

Background and factors considered

There have been conflicting views in the health sector regarding how Electronic Health Records (EHRs; these are referred to as Northern Ireland Electronic Care Records or NIECRs in Northern Ireland; hereafter EHRs) should be accessed and the patient data extracted for use in clinical trials. MHRA has asked the Innovation Hub to work with them to clarify the process and encourage best practice. The ICO's focus is on accountability, data accuracy, security and the minimisation of risk, in particular risk of data breach and data loss. It is to be hoped that the inclusion of adequate safeguards may reassure and potentially increase patient participation in clinical trials.

In producing this advice the ICO Innovation Hub hopes to give the sector confidence in facilitating access to EHRs for this beneficial work and to emphasise the need and long-term value of improving systems in the health sector in all parts of the UK. The potential held in EHRs needs systems fit for purpose if that potential is to be realised. Neither privacy legislation nor health legislation

prevent innovation - our mutual legislations describe what is necessary to build in compliance when patient data is used for purposes beyond direct care.

Assumptions and caveats

This advice to MHRA is written for the benefit of the Health Trust or Health Board or Donor (hereafter, the 'Health Trust') holding the EHRs who is facilitating access to the patient records they hold.

The organisation or Sponsor commissioning the clinical trial (hereafter, the 'Sponsor') will have their own responsibilities regarding patient data. These responsibilities are not considered here except where they directly affect the Health Trust holding the EHRs, though the advice provided here may be helpful for advising them about how to plan their own work.

Legal bases for accessing patient data for research are not covered in this advice.

Response

As a regulator advising Health Trusts on how to facilitate access to EHRs for clinical trials, MHRA may wish to raise the following points regarding GDPR compliance for contracts and data sharing agreements, data protection impact assessments and prior consultations, fines, accountability, and the security of the accessed data.

1 Contracts and data sharing agreements

Health Trusts need to know that a contract should be in place between themselves and the organisation carrying out the clinical trial. The contract should clearly set out the GDPR compliance standards the Health Trust expects from the Sponsor carrying out the clinical trial and any Processor they may use. The contract should, for example, stipulate the Processor's responsibilities regarding the deletion or return of patient data when the clinical trial has ended, as stipulated in Article 28(3)(g).

If the Sponsor is using another organisation as Processor (collecting the data on their instructions) a contract should also be in place between them which reflects the standards set by the Health Trust.

A contract alone will not cover the Health Trust's obligations under the GDPR - please see the sections on *accountability* and *security* in this advice for further information.

Using a Processor does not absolve Sponsors or Health Trusts of their responsibilities as Controllers under the GDPR. There is a responsibility to ensure Processors understand what is required of them and their obligations under the legislation.

2 Data Protection Impact Assessments (DPIAs)

The GDPR states that a DPIA will be required *before* processing starts where that processing is likely to result in a high risk to the rights and freedoms of individuals - see Article 35(1). This requirement is likely to engage EHRs in situations including:

-large scale processing of special category data (which includes data concerning health, sexual orientation, or data revealing racial or ethnic origin, religious beliefs or genetic data) as stated in Article 35(3)(b)

-the processing of genetic data

-the processing of vulnerable individuals' data (which would include patients)

-the processing of sensitive data

From the examples above it can be seen that a DPIA is likely to be mandatory in most cases for any Controller processing the data in EHRs, whether they are the Health Trust or the Sponsor of the clinical trial. The DPIA should document the proposed processing and the measures which will be taken to protect the rights and freedoms of individuals - this may include steps such as anonymisation or pseudonymisation. The risk assessment should conclude with a consideration of the likelihood and severity of any potential harm to individuals. The DPIA should also document how the Controller intends to meet their general compliance obligations under the GDPR.

Whilst Article 35(1) states that a single DPIA can cover a set of *similar* operations presenting *similar* risks, it will still be necessary to document why the decision was made to rely on an existing DPIA. Given the intrinsic value of carrying out a DPIA, the decision to rely on a previous assessment should not be taken lightly. A DPIA should never be reduced a mere box-ticking exercise. It may be helpful when advising Health Trusts to stress that conducting a DPIA is time well spent which actively reduces the risk of harm to patients and their personal data, building in GDPR compliance standards from the very start. Relying on a Sponsor's DPIA alone is not recommended, particularly if the Health Trust has not had the opportunity to scrutinise it.

Health Trusts should be made aware that the timing of a DPIA is critical, as they may need to allow time for prior consultation. DPOs should be consulted for advice about the intended processing and their response documented in the DPIA - see Article 35 (2).

Your advice could highlight the benefits of discussing the intended processing with the organisation commissioning the trial and any Processor they intend to use as this may highlight new areas of risk to consider in the DPIA. In particular, you could note that a discussion regarding the methods to be used may be helpful.

Publishing DPIAs can assist with the transparency requirement of the GDPR, developing trust and confidence in how organisations manage and appropriately share data in the public interest.

Prior consultations

Processing which presents a high risk to the rights and freedoms of individuals (or a moderate risk to a large number of individuals) can be mitigated by steps taken by the Controller, as set out in their DPIA. However, where the Controller identifies a residual high risk which *remains after* these steps have been taken, you should advise Health Trusts to contact the ICO for advice (prior consultation) before processing starts - see GDPR Article 36(1) and particularly Recital 94.

Health Trusts should be made aware that a response from the ICO may take up to eight weeks, with an option to extend to fourteen weeks, depending on the complexity of the intended processing. They will need to allow sufficient time to seek this advice.

Enforcement action and fines

In the advice it would be appropriate to mention the fines associated with DPIAs to ensure Health Trusts are familiar with them. Failing to carry out a DPIA or producing a DPIA which is inadequate may result in enforcement action and a significant fine - up to 10 million Euros or 2% of global annual turnover*, whichever is higher* - see Article 83(4)(a). The same fines apply if a prior consultation was necessary but was not carried out.

For more information on DPIAs please see the guidance on the ICO website and the website of the European Commission: ICO basic guidance; ICO detailed guidance; European Commission guidance on processing likely to constitute a high risk.

3 Accountability

GDPR makes accountability (the ability to demonstrate adherence to the GDPR and its principles) explicit in GDPR Article 5(2). Controllers must be able to demonstrate how they are meeting the obligations placed on them by the legislation.

It will be helpful for Health Trusts to consider the different methods of protecting patient data which could be put into place. The

data protection principles listed in Article 5(1) of the GDPR are an ideal place to start: adherence to principle c (data minimisation) will ensure that only the patient data necessary for the clinical trial is processed.

Data accuracy is addressed in principles d (accuracy) and f (integrity and confidentiality, security).

In demonstrating accountability to the data protection principles, the advice could suggest that measures are implemented to keep patient data secure and reduce risk. I have included suggestions below for consideration, which should be adapted by MHRA according to your knowledge of the sector and their relevance and appropriateness to the context. Whilst Health Trusts may wish to focus on organisational measures this approach has its limitations, which will be considered below. Measures should be appropriate to the potential impact of harm on patients if their data is accessed inappropriately, lost or inappropriately disclosed. Given that most of the data in a clinical trial will be special category data, the negative impact on individuals is likely to be high as it risks disclosure of an individual's health status.

Technical measures to protect the patient data might include the use of access controls on the IT systems used to hold EHRs. Depending on the state of the art available, the access controls could include restriction by individual or by staff roles as well as the ability to restrict the data fields viewed within the EHR.

Other preventative measures such as pseudonymisation will encourage the 'data protection by design and by default' approach to processing described in Article 25, which may help to limit the risk of data exposure in the event of a breach.

Organisational measures to protect the patient data might include the data sharing agreement setting out what is expected from external staff accessing EHRs for clinical trials, and staff training to ensure they are well-supported in their daily work, including how to use IT systems compliantly and to their fullest potential. Training and support should include what to do in the event of a data breach (particularly in the event of data loss and inappropriate data sharing), with clear instructions about who staff should contact regarding the breach in the first instance and any immediate steps which need to be taken.

Reliance on organisational measures alone is ultimately a reliance on goodwill alone - it may not provide the reassurance Health Trusts need that the EHRs they hold are adequately protected from serious internal or external threats.

Detective measures might include ensuring access to EHRs is auditable during the course of the clinical trial. This could be facilitated, for example, by ensuring that staff do not share their log-ons to access the EHRs. Auditable access during the course of the clinical trial provides an opportunity to regularly check that data access is compliant with the GDPR and the standards and expectations set out in the data sharing agreement.

The role of the monitor

The monitor is ideally placed to carry out checks to ensure that Controllers and Processors meet their responsibilities under the GDPR.

4 Security of the accessed data

Article 5(1)(f) of the GDPR stresses the importance of keeping personal data secure. It states that personal data should be:

'Processed 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, using appropriate technical or organisational measures'

MHRA have made the ICO aware that some Health Trusts print out the EHRs of patients participating in clinical trials as paper copies. We have been advised that this step is being taken as an alternative to allowing restricted or, in particular, unrestricted access to EHRs. In light of Article 5(1)(f) this cannot be seen as best practice for keeping personal data secure and preserving the integrity of the data.

Printing out an EHR risks the loss of some or all of the data in transit, creating a risk of inappropriate disclosure and data breach as well as possible enforcement action. When paper patient records are lost (or found in places where they are not supposed to be) there is a significant impact on public trust. If patients are not confident that their data will be kept secure it may hinder their willingness to participate in clinical trials.

Printed data may also be out of date due to the time taken to collate it, or incomplete due to incompatibilities in the IT system, which would increase the risk of breaching Article 5(1)(d) (accuracy) and may have a negative impact on the clinical trial. Re-entering data from printed records also increases the risk of the data being inaccurate or out of date.

Ultimately, IT systems fit for the future will support precision in data access and data protection by design and by default.

Advice provided by **Maddy Griffiths**	**Effective date** **30/03/2020**

ICO Innovation Hub

Terms and Conditions

1. Scope of the ICO's Regulators' Business Innovation Privacy Hub ("the Hub")

1.1 These terms and conditions include any terms set out in the Hub confirmation letter (together the "**Terms and Conditions**").

1.2 The support offered by the ICO ("**we**", "**us**"), to you, the organisation ("**you**", "**your**", or "**participant**") through the Hub is solely in relation to the proposition for an innovative product or service, outlined in the Hub confirmation letter (the "**Proposed Innovation**"). The direct benefits provided by us via the Hub can only be applied to innovations, products or services to the extent that they are offered or provided in the United Kingdom. We will be working in conjunction with [NAME] (your "**Regulator**"). The Hub confirmation letter sets out how we, you and your Regulator will work together. By signing the confirmation letter, you are agreeing to enter into a legally binding agreement with us, on the terms set out in the Terms and Conditions, and in consideration of the obligations each party has agreed to in the Terms and Conditions.

1.3 We will use our reasonable skill and care in providing our feedback, steers, guidance or other advice concerning the Proposed Innovation ("**Feedback**"), whether that Feedback is provided directly to you or via your Regulator. Unless we expressly document otherwise, our Feedback will be based on the specific information that you and/or your Regulator share with us and our understanding of the UK data protection law framework in force at the time. Only specific data protection law issues are open to our regulatory feedback and support through the Hub and we are not responsible for offering advice or support in relation to other regulatory aspects concerning the Proposed Innovation.

1.4 As a result, our Feedback should not be viewed as a full examination or audit and will not identify all of the risks associated with the Proposed Innovation, your activities or all possible areas of non-compliance. This remains the case even if we raise issues that you have not expressly brought to our attention.

1.5 You and we agree to co-operate to help you and us get the most out of your participation in the Hub. You agree to remain open and transparent with us at all times in relation to the Proposed Innovation including before, during and after the time we are working with you in the Hub. If you are aware of any information that you believe would affect our position, you must inform us immediately.

1.6 You agree that you remain responsible for your compliance with all legal and regulatory obligations, whether in respect of data protection law or otherwise. You warrant and undertake that you and your Proposed Innovation are, and will remain during the period you are receiving support from the Hub, in compliance with all applicable legal and regulatory obligations.

1.7 You are not required to comply with the Feedback, and you are always free to take your own independent legal advice. Of course, if you choose not to follow our Feedback you might not be able to continue working with us in the Hub, and you might be acting in breach of data protection law.

1.8 The Feedback is to you only and is specific to your circumstances. Except for your Regulator, it must not be shared with any other party (either in part or in full) without our express written permission. This does not prevent you from disclosing the Feedback to your employees, agents, consultants, advisors, representatives or sub-contractors, provided that:

(i) they are subject to obligations to maintain the confidentiality of the advice and not to disclose it to third parties; and

(ii) the Feedback is only used for the purposes of advising or assisting you.

1.9 Any Feedback is given without prejudice to any decision or action that we may take against you in the future, including any enforcement or other regulatory action. The positions reflected in the Feedback may change over time, for example on receipt of further information by us, or following a change in law, court judgments, regulatory guidance or ICO policy. It is important that you keep up to date with all relevant data protection law, guidance, policies and decisions of the courts after you leave the Hub, and it is entirely your responsibility to determine whether the Feedback requires updating due to such developments.

1.10 As mentioned in the Hub confirmation letter, working with the Hub does not prevent regulatory action by us or by any other competent data protection authority or by any other regulatory body or authority. The Feedback does not affect rights conferred on third parties (such as your customers), nor does it bind any courts, and may not reflect the views of the European Data Protection Board or any other data protection authority.

Lead organisation (where applicable)

1.11 Where you are acting as a lead organisation, and the development of the Proposed Innovation is shared among the persons and organisations listed below, you acknowledge and agree that our relationship in relation to the Hub is only with you and that we have no liability whatsoever to any of the third parties listed in clause 1.12 below (if applicable). You agree to indemnify us from and against any claim or complaint brought by a third party, including those listed below, under or in relation to these Terms and Conditions, your work with the Hub and/or the Proposed Innovation.

1.12 List of persons and organisations you are working with on the Proposed Innovation:

(i) [Add name, address and company number (if applicable)].

Safeguards

1.13 Where relevant, while you are working with the Hub we may require that you adopt safeguards to protect the rights of data subjects. We will determine the appropriate safeguards on a case-by-case basis, with the aim of ensuring that protections are sufficient, but at the same time not unnecessarily burdensome on you, considering your activities. Failure to implement any such safeguards or protections may result in your support from the Hub being terminated in line with these Terms and Conditions, and/or in our taking formal enforcement action against you, in line with our statutory powers as a regulator.

2. The scope of our role in the Hub

2.1 We will use reasonable care in our dealings with you in relation to the Hub and your Proposed Innovation. However, given the nature of the Hub and of our Feedback (and subject to clause 2.2), we do not accept any liability or responsibility for: (i) any opinions expressed or information included in any of our Feedback; (ii) the time it may take for us to provide any Feedback; and/or (iii) any other liability under or in relation to the Hub, the Proposed Innovation or these Terms and Conditions, whether in contract, tort (including negligence) or otherwise.

2.2 Nothing in these Terms and Conditions seeks to limit our liability in any way which is not permitted by law, including our liability to you for fraud or fraudulent misrepresentation.

3. Term of the Hub

3.1 You may continue to receive support from the Hub until and unless our relationship with you is ended in accordance with this clause 3, and/or if later, you receive a closing communication from us regarding the Hub.

3.2 Either you or we may at any time, on two week's written notice, terminate your involvement with the Hub.

3.3 We may, at any time terminate, with immediate effect, your involvement with the Hub and cease providing Feedback and any other regulatory support if: (i) you commit a material or repeated breach of these Terms and Conditions, which is not capable of remedy; or (ii) we (acting reasonably) determine that your conduct, either in involvement with or outside of the Hub, is contrary to the public interest or is likely to bring us into disrepute; or (iii) we cease to operate the Hub for any reason.

3.4 You acknowledge that due to the highly innovative nature of the Hub, we are entitled to suspend or terminate your work with the Hub at any time should the Hub trigger detrimental unexpected consequences for us, participants or data subjects.

3.5 Upon termination of your involvement with the Hub or where you receive a closing communication from us pursuant to clause 3.1, the Terms and Conditions will automatically terminate, save that the following clauses will survive termination or expiry, howsoever arising: clauses 2, 3, 4, 5, 6 and 8.

4. Intellectual property

4.1 You (and/or your licensors) will retain all intellectual property rights in, and responsibility for, all content and materials that you contribute to the Hub, which were in existence prior to the date that the Terms and Conditions came into effect and/or which you develop outside of your work with the Hub ("**Existing Intellectual Property**"). You will only submit Existing Intellectual Property that you have the right to share, use and develop, and you will fully comply with any third party licenses relating to the Existing Intellectual Property.

4.2 All intellectual property rights obtained, created or developed by you relating to your Proposed Innovation during your participation in the Hub ("**New Intellectual Property**") will vest in you, subject to any contrary agreement you may have with a third party.

4.3 We may use Existing Intellectual Property and New Intellectual Property as is reasonable to enable us to exercise our rights and perform our functions or obligations in connection with the Hub ("**Use**"), and you grant or must procure the grant of royalty-free and non-exclusive licences to us to Use the Existing Intellectual Property and the New Intellectual Property for the duration of the Terms and Conditions.

4.4 You warrant and undertake to ensure that the Use by us of any Existing Intellectual Property and/or New Intellectual Property will not infringe the rights of any third party.

4.5 You agree to defend, indemnify, and hold us harmless from and against any liability or loss (including, without limitation, any legal costs) incurred by us as a result of, or in connection with, our Use of Existing Intellectual Property and/or New Intellectual Property, including where the Existing Intellectual Property and/or New Intellectual Property infringe the rights of any third party.

5. Confidentiality

5.1 You must clearly identify to us, in writing, which information you provide to us that you consider to be your confidential information and provide clear reasons why you regard such information to be confidential ("**your confidential information**"). We will protect your confidential information as we do our own commercially sensitive information.

5.2 During the term of your work with the Hub and for so long as your confidential information remains confidential in nature and not available to the public, we will not use or disclose your confidential information without your prior written consent: (i) other than to provide Feedback or other support in connection with the Hub or to fulfil any of our functions or obligations, including as set out in this clause 5; and/or (ii) unless permitted or required to do so by law, statutory directions, court orders or government regulations.

5.3 We may use information obtained from you (including your confidential information) to help develop and provide guidance, policies and resources (on an anonymised basis) to the public.

5.4 We may disclose your confidential information to our employees, agents, consultants, advisors or representatives to the extent that such disclosure is reasonable in relation to the Hub, including for us to provide Feedback, and for the purposes set out in this clause 5, provided always that such employees, agents, consultants, advisors or representatives are made aware of and comply with the obligations of confidentiality under these Terms and Conditions.

5.5 We may disclose any information received from or relating to you, including your confidential information, to any regulator or public body in the UK or elsewhere (including, without limitation, the Centre for Data Ethics and Innovation), where such disclosure by us is made for the purposes of: (i) facilitating the performance of our functions; and/or (ii) complying with any specific legal or regulatory obligation.

5.6 We are bound by the Freedom of Information Act 2000 and as such can be asked to disclose certain information that we hold. We will endeavour to let you know if we are asked to share any information that relates to you and will seek to apply relevant exemptions from disclosure where appropriate.

5.7 Should you receive any confidential information belonging to us, you will keep that information confidential and only use it for the purpose for which it was provided to you. You will protect that confidential information as you do your own confidential information. At any time, at our request you shall securely return or securely destroy our confidential information in your possession or control. The obligations in this clause 5.7 shall continue during the term of the Hub and for so long afterwards as that confidential information remains confidential in nature and not available to the public.

5.8 Nothing in this clause 5 shall prevent us from using any techniques, ideas or know-how gained during the performance of these Terms and Conditions in the course of our normal business to the extent that this use does not result in a disclosure of your confidential information or an infringement of your Existing Intellectual Property and/or New Intellectual Property.

6. Communications relating to the Hub

6.1 The fact that you are receiving support from the Hub is not your confidential information, and we are able to disclose this fact as we consider it appropriate. Subject to clause 6.2, we will only publicise details of the support you receive from the Hub with your prior consent (not to be unreasonably withheld or delayed).

6.2 We may also, at our discretion, make public anonymised, aggregated information on the Hub and its participants.

6.3 Your involvement with the Hub does not represent an approval or endorsement by us of you or your Proposed Innovation. Neither you nor anyone acting on your behalf may publicise, nor make any statement or announcement, either expressly or by implication, that suggests that we have approved, endorsed, or otherwise accepted that you or your Proposed Innovation complies with regulatory requirements as a result of your involvement with the Hub.

6.4 Your organisation is not permitted to communicate to any third party that you are working with the Hub, before, during, or after the period you are receiving support from us in the Hub, without our express written and specific consent. This includes, but is not limited to, communications to any organisation, media outlet, existing or future customers, and data subjects.

7. Privacy and data protection

7.1 Unless otherwise agreed, any personal data (such as your staff contact details) provided to us as part of your work with the Hub will be processed by us as a data controller in line with our privacy notice.

7.2 You are responsible for providing a copy of our privacy notice to any employees or other data subjects whose personal data you share with us during your work with the Hub and you should ensure that such personal data is collected fairly and lawfully.

7.3 Given that we will only be processing minimal amounts of business-related personal data in relation to your work with the Hub, we do not at this stage deem it necessary to enter into a separate data sharing agreement with you. However, you must ensure that any transfer of personal data to us is completed in compliance with applicable law (including applicable data protection law).

7.4 We will implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including from unauthorised or unlawful processing of personal data, or accidental loss or destruction of, or damage to, that personal data, and will process all personal data received from you in compliance with the provisions and principles set out in data protection legislation.

7.5 You acknowledge and agree that your involvement with the Hub does not affect your responsibility or liability if personal data is corrupted, damaged or improperly used or disclosed by you.

8. General

8.1 Your involvement with the Hub does not create a joint venture, co-ownership, partnership or agency relationship between you and us. Neither you nor we will have the authority to incur, assume, or create, orally or in writing, any liability, obligation, or undertaking of any kind in the name of, or on behalf of, or in any way binding upon, the other.

8.2 We retain the right to amend these Terms and Conditions at any time by giving you reasonable notice in writing.

8.3 General words within these Terms and Conditions must not be given a restrictive meaning simply because they are followed by particular examples intended to be embraced by the general words.

8.4 Only you and we have rights under these Terms and Conditions. A person who is not a party to these Terms and Conditions has no rights to enforce it or enjoy any benefits under it, whether under the Contracts (Rights of Third Parties) Act 1999, or otherwise.

8.5 These Terms and Conditions, including the Hub confirmation letter, constitute the whole and only agreement between us and you relating to your involvement with the Hub. You acknowledge that you have not relied on any representation made by us or on our behalf which is not set out in these Terms and Conditions. If there is any conflict between any other communications from us and the terms set out in this document, the terms set out in this document will prevail.

8.6 Remedies under these Terms and Conditions are cumulative and may be exercised concurrently or separately.

8.7 If any provision of the Terms and Conditions is prohibited by law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from the Terms and Conditions without modifying the remaining provisions.

8.8 Any waiver or relaxation, either partly or wholly, of any of the Terms and Conditions shall be valid only if it is communicated to the other in writing and expressly stated to be a waiver, and shall not constitute a waiver of any right or remedy arising from any other breach of the Terms and Conditions.

8.9 Any formal notice to be given under the Terms and Conditions shall be in writing and may be served by personal delivery, first class recorded post, e-mail to the address of you or us (as applicable) set out in the Hub confirmation letter, or such other address as you or we have notified to other for formal notices. Notices shall be deemed served on the next working day after delivery. An email shall be deemed delivered when sent unless an error message is received or, where an out of office message is received, on the date the out of office message states the recipient is to return.

8.10 Any matter, claim or dispute arising out of or in connection with these Terms and Conditions, whether contractual or non-contractual, is to be governed by and determined in accordance with English law. You and we irrevocably submit to the jurisdiction of the English courts.

From: FOIA s.40(2)
To: Maddy Griffiths
Subject: RE: ICO to MHRA - Sponsor Access to EHRS - update
Date: 05 October 2020 07:54:31
Attachments: image001.jpg

External: This email originated outside the ICO.

Hi Maddy

No problem, I completely understand. I'm still waiting for the re-structured version from HRA – I'm sure you understand that this is lower priority than the COVID19 work and the Brexit work at the moment. Happy to share the next draft when I receive it as your advice is really helpful. Hope you are still doing OK?

FOIA s.40(2)
[redacted]
Expert Inspector, GCP
FOIA s.40(2)
[redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

From: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Sent: 02 October 2020 19:25
To: FOIA s.40(2)
Cc: Sarah Meyers <Sarah.Meyers@ico.org.uk>
Subject: ICO to MHRA - Sponsor Access to EHRS - update

Dear FOIA s.40(2)

I have been speaking to my manager regarding this piece of work, who has advised me that whilst the ICO are able to offer advice to organisations we are not, unfortunately, able to produce joint advice. This has been a misunderstanding on my part, but it is due to the ICO's position as a regulator regarding personal data (which is a consideration for many sectors) rather than a regulator for a specific sector (such as MHRA).

This doesn't mean I can't help regarding this advice, but it does mean that it cannot be presented as joint advice from the ICO.

I appreciate this may be frustrating at this late stage of our discussions but the fault is entirely mine. I'm happy to give feedback on any further drafts of the advice, which was agreed to be redrafted by HRA following

our last meeting.

Please do feel free to call me if it would be helpful too.

All my best wishes,

Maddy.

Maddy Griffiths
Senior Policy Officer - Innovation Hub Technology and Innovation
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6303
ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For information about what we do with personal data see our privacy notice

From: FOIA s.40(2)
To: Maddy Griffiths
Subject: Monitors access to EHRs
Date: 16 October 2020 14:23:53
Attachments: DPIA and Access to EHR by Sponsor in clinical trials_16 Oct 2020.docx

---

External: This email originated outside the ICO.

Hi Maddy

We think we have a document that reflects where we got to at our last meeting, so MHRA and HRA are happy with this version. Can you please take a look from the ICO point of view and let me know if you have any comments?

Have a lovely weekend

FOIA s.40(2)
[redacted]
Expert Inspector, GCP
FOIA s.40(2)
[redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

Data Protection Impact Assessments in Clinical Trials

UK Guidance

Introduction

The following guidance has been jointly developed by HRA and MHRA, in consultation with ICO, on behalf of the UK.

The Data Protection Act 2018 states that "Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment." (DPIA) (Article 64(1)).

For personal data processed for the purpose of a healthcare research project, the sponsor of the project is the controller and the participating NHS organisation is their processor[1]. As such, DPIAs for the processing of personal data that is undertaken for the purpose of research are the responsibility of the sponsor.

Organisations that regularly sponsor research projects should undertake their DPIA(s) at the level of the Quality Management System, by the policies, processes, systems, etc. by which they design and manage their research portfolios (i.e. sponsors should operate on the basis of data protection by design, ensuring that their sponsor processes create compliant research projects, rather than attempting to work only reactively, on a study by study basis).

Expectations

Individual projects should be designed and delivered in accordance with the sponsor processes that are already subject to DPIA. The sponsor should have checks in place to satisfy itself that each study is compliant, by virtue of the fact that the study has been designed and will be delivered in accordance with the processes already subject to DPIA. Where the study deviates from the established processes (for example, where it is intended that a project uses a new technology for the processing of personal data, or requires that safeguards set out in standing policies cannot be applied), the sponsor should consider whether a study specific DPIA is appropriate, or (more likely) whether existing DPIA(s) should be revisited.

Although participating NHS organisations are not responsible for the DPIA of the processing activities that they will undertake on behalf of research sponsors, they are responsible for ensuring that they process data only in accordance with appropriate technical and organisational measures. Where sponsors are to rely upon existing NHS processes, systems, etc. for the processing of personal data (as opposed to when study specific provisions are required by the sponsor, e.g. eCRF) the sponsor should take assurance, that the measures taken by the NHS are appropriate, from the fact that their processor is an NHS organisation, i.e. from the high standards of data protection to which NHS organisations are held in each of the four UK nations.

To support the assurance to sponsors noted above, all NHS organisations should ensure that their policies, processes, systems, etc., upon which their processing of personal data depends,

[1] The controller is the party that determines the purpose and means of the processing (GDPR Article 4(7)) and the sponsor is the party that takes overall responsibility for the research (Policy Framework for Heath and Social Care, 9.10). Whilst the sponsor may take advice from other parties in determining the means and purpose of the data processing, it is ultimately responsible for deciding whether and how to act upon that advice. For further general guidance on data protection in healthcare research please see https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/

take proper account of their foreseeable use in processing personal data for research. NHS organisations should ensure that their own DPIAs, at the organisational, sub-organisational and/or individual system (e.g. electronic health records) level, explicitly account for participation in research, including projects sponsored by external organisations.

As with DPIA expectations on sponsors, an approach to data protection by design, including proper consideration of research specific needs, should ensure that individual studies need only be assessed for fit with anticipated requirements, already accounted for in local DPIA. The need to undertake more detailed project specific evaluation and provide bespoke arrangements should be reduced to an absolute minimum in this fashion.

In the case of both sponsors and participating NHS organisations, the expectation that individual studies are checked against existing arrangements does not replace the requirement that those arrangements are themselves regularly revisited (e.g. sponsors should ensure that their systems and processes are regularly reviewed to ensure that they, and their associated DPIAs, remain fit for purpose. Participating organisations should similarly regularly revisit their DPIAs and in so doing take account of any changes in foreseeable research needs, e.g. the move to more remote access to EHR for study monitors).

On-Site Access to Electronic Health Records by Sponsor Representatives in Clinical Trials

UK Guidance

Introduction

The following guidance has been jointly developed by HRA and MHRA, in consultation with ICO, on behalf of the UK.

The data collected and analysed during clinical trials are of course vital to preventing or treating diseases. These data are verified and overseen by clinical trial Sponsors via representatives such as Clinical Research Associates (CRAs) or monitors, who will review the medical records to ensure that they match the data collected by the Sponsor, via Source Data Verification (SDV). The trial participants consent to this access of their medical records in writing, as part of the consent to take part in the clinical trial.

Increasingly, medical records are now electronic (Electronic Health Records; EHRs) and this poses challenges in terms of direct access by the monitor/CRA to these records, ensuring that access is restricted to only those participants in the trial, and not any other patients whose records are maintained in the same system. Historically, monitors could be provided with the physical records of individual trial participants, without also providing them access to the records of other patients. Where EHRs have been designed to allow similarly restricted access, access may continue to be provided as it has been. Where EHRs do not have this functionality, additional safeguards are required.

Expectations

Provision of research monitor access to EHRs should be an integral part of organisational level (or EHR level) planning and risk assessment (**see accompanying joint advice on DPIA**) and, where at all possible, risks should be mitigated by EHR system design that ensures research monitor access is limited to only the records of specified relevant clinical trial participants and that this access is auditable

Where EHR systems have not been so designed, remedial action should be instituted at the next system update, to provide for monitor access limited to specified patients.

Where EHR systems are not yet able to restrict monitor access to the records of only their clinical trial participants, resorting to printouts from the EHR is not an appropriate mitigation or safeguard. **This system shortcoming should be addressed in organisation (or EHR) level risk assessment and short-term mitigations implemented pending system update**.
Such mitigations should include:

- Reliance upon the information governance obligations imposed upon sponsors and their representatives by the model agreements (mCTA, etc.), e.g.
    - Monitors should be provided with access to EHR (such access constituting processing) in accordance with the template agreement that requires that they understand their responsibilities for information governance, including their obligation to process the data of clinical trial participants securely, and to only disseminate or disclose for lawful and appropriate purposes.
    - That monitors hold employment contracts (with the sponsor, CRO, or authorised delegate) providing for personal accountability and sanctions for breach of confidence or misuse of data including deliberate or avoidable personal data breaches, which would include accessing EHR data of persons other than relevant clinical trial participants.

  N.B. it is not appropriate or necessary to enter into further non-disclosure agreements with the sponsor or its corporate or individual representatives;

- Standard training for monitors on use of the specific EHR, to cover actions to be taken in the event of any inadvertent breach

Where this restricted access is not possible MHRA has seen that some NHS Organisations have instead been printing out medical records for monitors to review. MHRA Inspectors have encountered several issues with this approach, for example; information is not always available, as medical histories have been incomplete and important information has been missing, due to the printed report settings. MHRA has seen gaps in printouts as reports are generated from one date to another and these are not always continuous; in some cases, this has resulted in weeks of missing data and also missing safety information. Additionally, information can be held in annotations in the systems that are also not printed out, such as causality assessment for adverse events. The practice of printing out these records also places a burden on the investigator sites.

Printing out an EHR risks the loss of some or all of the data should it need to be moved within the site, creating a risk of inappropriate disclosure and data breach as well as possible enforcement action. Printed data may also be out of date due to the time taken to collate it, or incomplete due to incompatibilities in the IT system, which would increase the risk of breaching GDPR and may have a negative impact on the clinical trial. When paper patient records are lost (or found in places where they are not supposed to be) there is a significant impact on public trust. If patients are not confident that their data will be kept securely, it may hinder their willingness to participate in clinical trials

From: FOIA s.40(2)
To: Maddy Griffiths
Subject: RE: ICO to MHRA - Monitors access to EHRs - feedback on the new draft - positive!
Date: 28 October 2020 08:50:39
Attachments: image002.jpg
image003.jpg
DPIA and Access to EHR by Sponsor in clinical trials_26 Oct 2020.docx

---

External: This email originated outside the ICO.
Hi Maddy – that's great – FOIA s.40(2) has tweaked according to your comments, so I'm now going to go about getting it published on our website.
Thank you so much for your support on this, it's very much appreciated.
Best wishes

FOIA s.40(2)
Expert Inspector, GCP
FOIA s.40(2)
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

From: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Sent: 23 October 2020 23:17
To: FOIA s.40(2)
Subject: ICO to MHRA - Monitors access to EHRs - feedback on the new draft - positive!

Dear FOIA s.40(2)

Thank you for sending the updated draft of the advice regarding EHRs. It's a great document – well-organised and clear. (I tend to annotate a working copy when checking a document – in this case I covered it in positive comments!). As the changes I'm suggesting are small, I've included them here rather than as tracked changes on the original document.

I'd suggest referring to GDPR Article 35(1) first, then DPA 2018 Section 64(1) in the opening statement as GDPR is the main reference point regarding carrying out a DPIA:

The Data Protection Act 2018 states that "Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment." GDPR Article 35(1); ~~(DPIA)~~ DPA 2018 ~~Article~~ Section 64(1).

I'd also suggest (in light of Royal Free/Deep Mind):

Where the study deviates from the established processes (for example, where it is intended that a project uses a new technology for the processing of personal data, or requires that safeguards set out in standing policies cannot be applied), the sponsor should consider whether a study specific DPIA is appropriate to address the level of risk, or ~~(more likely)~~ whether updating existing DPIA(s) will be sufficient ~~should be revisited~~.

I don't want to suggest overburdening organisations – it's simply that Royal Free/Deep Mind had a significant impact on public trust at the time – a negative outcome which could have been mitigated by a carefully considered DPIA. As a champion of innovation, I want to make sure that innovative trials happen – and that sponsors and NHS organisations are adequately supported (rather than hindered) by processes such as a DPIA when they make decisions regarding access to patient data. (I appreciate that there is a difference in risk when the data accessed is that of patients who have volunteered for the trial – which wasn't the case in Royal Free/Deep Mind).

I particularly like:

NHS organisations should ensure that their own DPIAs, at the organisational, sub-organisational and/or individual system (e.g. electronic health records) level, explicitly account for participation in research, including projects sponsored by external organisations.

and

In the case of both sponsors and participating NHS organisations, the expectation that individual studies are checked against existing arrangements does not replace the requirement that those arrangements are themselves regularly revisited (e.g. sponsors should ensure that their systems and processes are regularly reviewed to ensure that they, and their associated DPIAs, remain fit for purpose. Participating organisations should similarly regularly revisit their DPIAs and in so doing take account of any changes in foreseeable research needs, e.g. the move to more remote access to EHR for study monitors.

as this approach will support staff in their daily roles and supports both sponsors and participating organisations in their awareness and opportunity to mitigate risk.

I'm currently discussing with colleagues regarding your kind invitation to join a stakeholder group to improve EHRs. When I have a response from them I will contact you.

FOIA s.40(2) [redacted]

All my best wishes,

Maddy.

Maddy Griffiths
Senior Policy Officer - Innovation Hub Technology and Innovation
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6303
ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For information about what we do with personal data see our privacy notice

---

From: FOIA s.40(2) [redacted]
Sent: 20 October 2020 13:44
To: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Subject: RE: ICO to MHRA - Monitors access to EHRs - checking the document

External: This email originated outside the ICO.
Hi Maddy – FOIA s.40(2) [redacted] All's well here – look forward to hearing from you later in the week
Best wishes
FOIA s.40(2) [redacted]
Expert Inspector, GCP
FOIA s.40(2) [redacted]
I,E&S/Library

National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

From: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Sent: 20 October 2020 13:22
To: FOIA s.40(2) [redacted]
Subject: ICO to MHRA - Monitors access to EHRs - checking the document

Hi Gail,

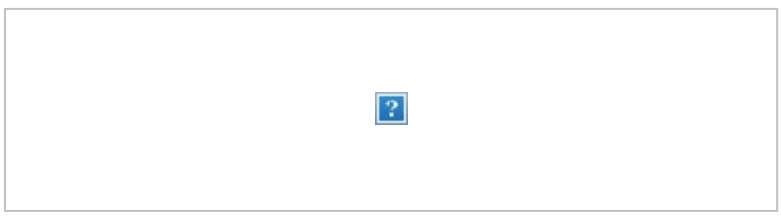
Lovely to hear from you.

FOIA s.40(2) [redacted] will be in touch with feedback ideally by the end of this week.

Hope all is well with you and your family,

Best wishes,

Maddy



Maddy Griffiths
Senior Policy Officer - Innovation Hub Technology and Innovation
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6303
ico.org.uk
twitter.com/iconews

From: FOIA s.40(2) [redacted]
Sent: 16 October 2020 14:23
To: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Subject: Monitors access to EHRs

External: This email originated outside the ICO.
Hi Maddy
We think we have a document that reflects where we got to at our last meeting, so MHRA and HRA are happy with this version. Can you please take a look from the ICO point of view and let me know if you have any comments?
Have a lovely weekend

FOIA s.40(2) [redacted]
Expert Inspector, GCP
FOIA s.40(2) [redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

Data Protection Impact Assessments in Clinical Trials

UK Guidance

Introduction

The following guidance has been jointly developed by HRA and MHRA, in consultation with ICO, on behalf of the UK.

The Data Protection Act 2018 states that "Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment." GDPR Article 35(1); DPA 2018 Section 64(1).

For personal data processed for the purpose of a healthcare research project, the sponsor of the project is the controller and the participating NHS organisation is their processor[1]. As such, DPIAs for the processing of personal data that is undertaken for the purpose of research are the responsibility of the sponsor.

Organisations that regularly sponsor research projects should undertake their DPIA(s) at the level of the Quality Management System, by the policies, processes, systems, etc. by which they design and manage their research portfolios (i.e. sponsors should operate on the basis of data protection by design, ensuring that their sponsor processes create compliant research projects, rather than attempting to work only reactively, on a study by study basis).

Expectations

Individual projects should be designed and delivered in accordance with the sponsor processes that are already subject to DPIA. The sponsor should have checks in place to satisfy itself that each study is compliant, by virtue of the fact that the study has been designed and will be delivered in accordance with the processes already subject to DPIA. Where the study deviates from the established processes (for example, where it is intended that a project uses a new technology for the processing of personal data, or requires that safeguards set out in standing policies cannot be applied), the sponsor should consider whether a study specific DPIA is appropriate to address the level of risk, or whether updating existing DPIA(s) will be sufficient.

Although participating NHS organisations are not responsible for the DPIA of the processing activities that they will undertake on behalf of research sponsors, they are responsible for ensuring that they process data only in accordance with appropriate technical and organisational measures. Where sponsors are to rely upon existing NHS processes, systems, etc. for the processing of personal data (as opposed to when study specific provisions are required by the sponsor, e.g. eCRF) the sponsor

[1] The controller is the party that determines the purpose and means of the processing (GDPR Article 4(7)) and the sponsor is the party that takes overall responsibility for the research (Policy Framework for Health and Social Care, 9.10). Whilst the sponsor may take advice from other parties in determining the means and purpose of the data processing, it is ultimately responsible for deciding whether and how to act upon that advice. For further general guidance on data protection in healthcare research please see https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/

should take assurance, that the measures taken by the NHS are appropriate, from the fact that their processor is an NHS organisation, i.e. from the high standards of data protection to which NHS organisations are held in each of the four UK nations.

To support the assurance to sponsors noted above, all NHS organisations should ensure that their policies, processes, systems, etc., upon which their processing of personal data depends, take proper account of their foreseeable use in processing personal data for research. NHS organisations should ensure that their own DPIAs, at the organisational, sub-organisational and/or individual system (e.g. electronic health records) level, explicitly account for participation in research, including projects sponsored by external organisations.

As with DPIA expectations on sponsors, an approach to data protection by design, including proper consideration of research specific needs, should ensure that individual studies need only be assessed for fit with anticipated requirements, already accounted for in local DPIA. The need to undertake more detailed project specific evaluation and provide bespoke arrangements should be reduced to an absolute minimum in this fashion.

In the case of both sponsors and participating NHS organisations, the expectation that individual studies are checked against existing arrangements does not replace the requirement that those arrangements are themselves regularly revisited (e.g. sponsors should ensure that their systems and processes are regularly reviewed to ensure that they, and their associated DPIAs, remain fit for purpose. Participating organisations should similarly regularly revisit their DPIAs and in so doing take account of any changes in foreseeable research needs, e.g. the move to more remote access to EHR for study monitors).

On-Site Access to Electronic Health Records by Sponsor Representatives in Clinical Trials

UK Guidance

Introduction

The following guidance has been jointly developed by HRA and MHRA, in consultation with ICO, on behalf of the UK.

The data collected and analysed during clinical trials are of course vital to preventing or treating diseases. These data are verified and overseen by clinical trial Sponsors via representatives such as Clinical Research Associates (CRAs) or monitors, who will review the medical records to ensure that they match the data collected by the Sponsor, via Source Data Verification (SDV). The trial participants consent to this access of their medical records in writing, as part of the consent to take part in the clinical trial.

Increasingly, medical records are now electronic (Electronic Health Records; EHRs) and this poses challenges in terms of direct access by the monitor/CRA to these records, ensuring that access is restricted to only those participants in the trial, and not any other patients whose records are maintained in the same system. Historically,

monitors could be provided with the physical records of individual trial participants, without also providing them access to the records of other patients. Where EHRs have been designed to allow similarly restricted access, access may continue to be provided as it has been. Where EHRs do not have this functionality, additional safeguards are required.

Expectations

Provision of research monitor access to EHRs should be an integral part of organisational level (or EHR level) planning and risk assessment (**see accompanying joint advice on DPIA**) and, where at all possible, risks should be mitigated by EHR system design that ensures research monitor access is limited to only the records of specified relevant clinical trial participants and that this access is auditable

Where EHR systems have not been so designed, remedial action should be instituted at the next system update, to provide for monitor access limited to specified patients.

Where EHR systems are not yet able to restrict monitor access to the records of only their clinical trial participants, resorting to printouts from the EHR is not an appropriate mitigation or safeguard. **This system shortcoming should be addressed in organisation (or EHR) level risk assessment and short-term mitigations implemented pending system update**.

Such mitigations should include:

- Reliance upon the information governance obligations imposed upon sponsors and their representatives by the model agreements (mCTA, etc.), e.g.
    - Monitors should be provided with access to EHR (such access constituting processing) in accordance with the template agreement that requires that they understand their responsibilities for information governance, including their obligation to process the data of clinical trial participants securely, and to only disseminate or disclose for lawful and appropriate purposes.
    - That monitors hold employment contracts (with the sponsor, CRO, or authorised delegate) providing for personal accountability and sanctions for breach of confidence or misuse of data including deliberate or avoidable personal data breaches, which would include accessing EHR data of persons other than relevant clinical trial participants.

  N.B. it is not appropriate or necessary to enter into further non-disclosure agreements with the sponsor or its corporate or individual representatives;

- Standard training for monitors on use of the specific EHR, to cover actions to be taken in the event of any inadvertent breach

Where this restricted access is not possible MHRA has seen that some NHS Organisations have instead been printing out medical records for monitors to review. MHRA Inspectors have encountered several issues with this approach, for example; information is not always available, as medical histories have been incomplete and

important information has been missing, due to the printed report settings. MHRA has seen gaps in printouts as reports are generated from one date to another and these are not always continuous; in some cases, this has resulted in weeks of missing data and also missing safety information. Additionally, information can be held in annotations in the systems that are also not printed out, such as causality assessment for adverse events. The practice of printing out these records also places a burden on the investigator sites.

Printing out an EHR risks the loss of some or all of the data should it need to be moved within the site, creating a risk of inappropriate disclosure and data breach as well as possible enforcement action. Printed data may also be out of date due to the time taken to collate it, or incomplete due to incompatibilities in the IT system, which would increase the risk of breaching GDPR and may have a negative impact on the clinical trial. When paper patient records are lost (or found in places where they are not supposed to be) there is a significant impact on public trust. If patients are not confident that their data will be kept securely, it may hinder their willingness to participate in clinical trials

From: FOIA s.40(2)
To: Maddy Griffiths
Cc: Sarah Meyers
Subject: RE: ICO to MHRA - EHR advice - final feedback!
Date: 04 November 2020 12:13:49
Attachments: image001.jpg
image003.jpg
image004.jpg
image005.jpg

External: This email originated outside the ICO.
Hi Maddy – that is great news, thank you so much for all your work on this.
Best wishes

FOIA s.40(2)
Expert Inspector, GCP
FOIA s.40(2)
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

From: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Sent: 04 November 2020 12:07
To: FOIA s.40(2)
Cc: Sarah Meyers <Sarah.Meyers@ico.org.uk>
Subject: ICO to MHRA - EHR advice - final feedback!
Importance: High

Hi FOIA s.40(2)

The last of the feedback is back – colleagues are happy with the document as it stands. (I thought they would be – but wanted to check).
There was a suggestion to make the final paragraph more person-centred – I've made a minor adjustment to the text:

> Printing out an EHR risks the loss of some or all of the data should it need to be moved within the site, creating a risk of inappropriate disclosure, distress and harm to patients, ~~and~~ data breach ~~as well as~~ and possible enforcement action. Printed data may also be out of date due to the time taken to collate it, or incomplete due to incompatibilities in the IT system, which would increase the risk of breaching GDPR and may have a negative impact on the clinical trial. When paper patient records are lost (or found in places where they are not supposed to be) there is a significant impact on public trust. If patients are not confident that their data will be kept securely, it may hinder their willingness to

participate in clinical trials.

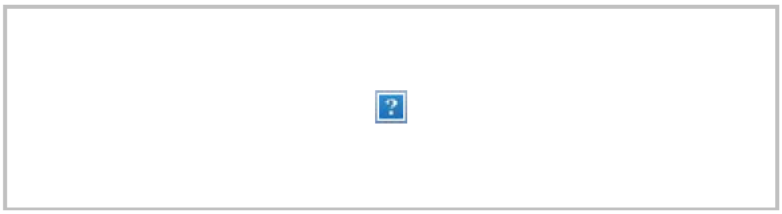
It's a tiny change, but it does flag the immediate impact on the individual rather than the impact on Controllers alone or more long term impact on the wider public, which I couldn't help but agree with!

I won't be accepting any more feedback from colleagues now so I'm happy for the document to be published – with or without the change given above. My apologies for the delay - I wanted to allow time for colleagues to respond.

It's a good document – I'm glad to have been part of this process.

All my best wishes,

Maddy.



Maddy Griffiths
Senior Policy Officer - Innovation Hub Technology and Innovation
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6303
ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For information about what we do with personal data see our privacy notice

---

From: FOIA s.40(2) [redacted]
Sent: 03 November 2020 07:58
To: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Subject: RE: ICO to MHRA - Request for temporary publication hold on EHR advice

External: This email originated outside the ICO.
Hi Maddy – any news?
Thanks
FOIA s.40(2) [redacted]

Expert Inspector, GCP
FOIA s.40(2) [redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

From: FOIA s.40(2) [redacted]
Sent: 29 October 2020 15:51
To: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Subject: RE: ICO to MHRA - Request for temporary publication hold on EHR advice

Hi Maddy – we are just going through internal clearance at the moment – can you let me know as soon as possible if there are any issues? Any idea when this might be?
Thanks

FOIA s.40(2) [redacted]
Expert Inspector, GCP
FOIA s.40(2) [redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

Read our guidance on coronavirus (COVID-19)

Stay connected: mhra.gov.uk/stayconnected
MHRA is a centre of the Medicines and Healthcare Products Regulatory Agency

---

From: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Sent: 29 October 2020 15:46
To: FOIA s.40(2) [redacted]
Subject: ICO to MHRA - Request for temporary publication hold on EHR advice
Importance: High

Hi FOIA s.40(2) [redacted]

My apologies – I've just had some feedback from colleagues in relation

to this advice. Would you mind putting publication of the advice on hold until I've picked through their views?

I'm so sorry to hold you up at this point!

Best wishes,

Maddy

Maddy Griffiths
Senior Policy Officer - Innovation Hub Technology and Innovation
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6303
ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For information about what we do with personal data see our privacy notice

---

From: FOIA s.40(2)
Sent: 28 October 2020 08:50
To: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Subject: RE: ICO to MHRA - Monitors access to EHRs - feedback on the new draft - positive!

External: This email originated outside the ICO.
Hi Maddy – that's great – FOIA s.40(2) has tweaked according to your comments, so I'm now going to go about getting it published on our website.
Thank you so much for your support on this, it's very much appreciated.
Best wishes

FOIA s.40(2)
Expert Inspector, GCP
FOIA s.40(2)
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare

From: FOIA s.40(2)
To: Maddy Griffiths
Cc: Sarah Meyers
Subject: RE: ICO to MHRA - advice on access to EHRs published!
Date: 10 December 2020 10:58:54
Attachments: image002.jpg

External: This email originated outside the ICO.

Thanks Maddy – you were a tremendous help, I learned a lot. The reason it was split really came down to our internal clearance process - it's a long story, but it was the easiest way to get it published in the end.

Best wishes

FOIA s.40(2)
[redacted]
Expert Inspector, GCP
FOIA s.40(2)
[redacted]
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire
EN6 3QG

From: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Sent: 09 December 2020 19:22
To: FOIA s.40(2) [redacted]
Cc: Sarah Meyers <Sarah.Meyers@ico.org.uk>
Subject: ICO to MHRA - advice on access to EHRs published!

Hi FOIA s.40(2) [redacted]

It's great to see that the finalised advice has been published. I've let the ICO's DPIA team know as they were very helpful in the early work on this project.
I was a little surprised to see that the 'all in one' advice had been split into two, sitting on two different websites. I understand completely that every regulator has a specific remit but hope you will forgive my long term aspiration that seamless advice benefitting from the input of more than one regulator will one day be easier to achieve than at present.
I'm really delighted to have been part of this work and hope my contribution to it was a help rather than a hindrance!

All my best wishes,

Maddy

Maddy Griffiths
Senior Policy Officer - Innovation Hub Technology and Innovation
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0330 414 6303
ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For information about what we do with personal data see our privacy notice

---

From: FOIA s.40(2)
Sent: 02 December 2020 10:34
To: Maddy Griffiths <Madelaine.Griffiths@ico.org.uk>
Subject: Access to EHRs by monitors

External: This email originated outside the ICO.
Hi Maddy - after a lengthy clearance process, we finally have the guidance for access to EHRs by monitors while onsite: https://www.gov.uk/guidance/good-clinical-practice-for-clinical-trials#on-site-access-to-electronic-health-records-by-sponsor-representatives-in-clinical-trials

The guidance points to the HRA page too, as this is where we put the part in relation to the DPIAs – this sits better on the HRA site.

Best wishes

FOIA s.40(2)
Expert Inspector, GCP
FOIA s.40(2)
I,E&S/Library
National Institute for Biological Standards and Control - A Centre of the Medicines and Healthcare Products Regulatory Agency
Blanche Lane
South Mimms
Potters Bar
Hertfordshire

EN6 3QG

Read our guidance on coronavirus (COVID-19)

The UK has left the EU, and the transition period ends on 31 December 2020. Click here to find out more.
If you have not done so, please register now for MHRA Submissions, so you are ready from 1 January 2021.

Stay connected: mhra.gov.uk/stayconnected
MHRA is a centre of the Medicines and Healthcare Products Regulatory Agency

---