NHS England
PO Box 16738
Redditch
B97 9PT

Publishing Approval Reference: 000120

21 February 2019

Dear Colleagues,

EU Exit and ensuring continued access to, processing and sharing of personal data

We are writing to provide guidance on the actions that NHS Organisations need to take in order to ensure continuity of access to, processing and sharing of personal data as part of the Government's contingency preparations for a 'No Deal' European Union (EU) exit. **This letter and the accompanying Q&As should be passed to your Data Protection Officer for urgent action.**

There are potential issues relating to the use of data following a 'No Deal' EU exit, which could include issues with the onward use of personal data where it is not disaggregated and with data flows, particularly from small suppliers. These issues are not insurmountable and can be addressed with appropriate prior action. This letter details the steps that need to be taken by organisations to ensure that they have taken appropriate steps to ensure data flows are not disrupted by a 'No Deal' EU exit, including the use of appropriate safeguards where these are required.

Each organisation is a data controller and therefore has its own legal obligation to meet the terms of the General Data Protection Regulations (GDPR). The EU Exit Operational Readiness Guidance, published by the Department of Health and Social Care (DHSC) in December 2018 advised that NHS organisations need to:

- Investigate your organisation's reliance on transfers of personal data from the EU/EEA to the UK, especially those that are critical to patient care and/or would have a serious impact upon the system if they were disrupted.

- Note that many organisations tend not to disaggregate personal and non-personal data. As such, please be aware that restrictions on personal data may have knock-on effects on data more generally.

- Follow the advice from The Department for Digital, Culture, Media and Sport and the ICO on data protection in a 'no deal' scenario, which can be viewed on Gov.uk and on the ICO website, in particular to determine where to use and how to implement standard contractual clauses.

- Ensure that your data and digital assets are adequately protected by completing your annual Data Security and Protection Toolkit assessment. This self-audit of compliance EU Exit Operational Readiness Guidance 24 with the 10 Data Security Standards is important anyway, and mandatory to complete by the end of March 2019, but completing it early will enable health and adult social care providers to more quickly identify and address any vulnerabilities.

NHS England and NHS Improvement have established local, regional and national teams to enable rapid support on emerging local incidents. **Issues and concerns should be reported to your regional EU Exit Inbox as early as possible**. In turn these regional teams can escalate issues to the EU Exit National Co-ordination Centre. This co-ordination centre feeds into the Operational Response Centre which has been established by DHSC.

You can contact your regional inbox using the following details:

Region	**EU Exit inbox**
North East	England.euexitnortheast@nhs.net
North West	England.euexitnorthwest@nhs.net
Midlands	England.mids-euexit@nhs.net
East of England	England.eoe-euexit@nhs.net
London	England.london-euexit@nhs.net
South East	England.se-euexit@nhs.net
South West	England.sw-euexit@nhs.net

Practical guidance, in the form of Frequently Asked Questions, is attached in order to explain some of the queries on how to approach the above actions for NHS organisations. The Frequently Asked Questions set out the potential implications for personal data when the UK leaves the EU, what can be done to prepare and how to put in place appropriate safeguards. You can actively prepare from now in readiness for leaving the EU on the 29 March 2019 and solutions can be put in place once the UK is no longer a member of the EU.

There are also some additional concerns which have been raised in relation to data flows which organisations need to address:

Data controller to data controller data flows
Data protection officers are being asked to identify flows of personal data that may be affected and to work with organisations in EEA countries to put in place the relevant appropriate safeguards.

Whilst there are potential impacts on personal data sharing, processing and access

from leaving the EU, it is important to note that a UK data controller and an EEA data controller can apply an 'appropriate safeguard' to enable personal data flows to continue. However, any safeguard used must be legitimate and there should be consistency across the health and social care system in their use and how they are applied.

The Information Commissioner's Office (ICO) has identified which safeguards are most appropriate in different circumstances. It should, therefore, not be necessary for health and adult social care organisations to establish for themselves, or to seek legal advice to identify those safeguards.

Data processor to data controller data flows

In a 'No Deal' EU exit the UK will become a non-adequate third country – i.e. a country with which the EU has no agreement on standards – until an adequacy decision is made. The European Data Protection Board (EDPB) is currently deliberating whether flows from an adequate EEA processor to a non-adequate controller should constitute a restricted international transfer. It is not likely to reach a determination before 29th March. Until such time as the EDPB rule upon the issue, it is viewed that these flows remain unrestricted and can continue to flow uninterrupted as they have for around 20 years.

There is a possibility that some smaller suppliers may not realise that these flows are unrestricted and would cease flows. There is no suggestion that larger suppliers would cease flows. Data controllers should identify what flows they have and speak to suppliers to assure the flow will continue. If no assurance is received, the data controller needs to assess the risk to patient care. If the flow is critical to patient care, as a last resort you should consider repatriation of the data. If considering repatriation, you should contact your regional EU Exit inbox.
NHS providers and commissioners will be supported by NHS England and Improvement local teams to resolve issues caused, or affected, by EU Exit as close to the frontline as possible.

We hope this information helps you to understand the work underway and to provide reassurance within your organisation.

Thank you for your continued support and work on this important issue.

Yours sincerely,

Dawn Monaghan
Head of Data Sharing and Privacy (NHS England)
Head of Strategic IG (NHS Digital) and Director Information Governance Alliance

Professor Keith Willett
EU Exit Strategic Commander
Medical Director for Acute Care & Emergency Preparedness

Frequently asked questions on Data Protection in a no deal EU Exit

Guidance is also available on the ICO website.

What is personal data?

"Personal data" is defined in the General Data Protection Regulation (GDPR) as: "information relating to an identified or identifiable natural person", as outlined in the ICO's guidance.

Which organisations are affected by 'no deal' on data protection?

Many public, private and voluntary organisations that handle personal data will be affected and should make themselves aware of the implications of exit.

All organisations are responsible for their arrangements for the continued protection and exchange of personal data.

What are the implications for sharing personal data if the UK leaves the EU without a deal and how can we prepare?

We are aware of concerns in the health and social care system about how to ensure that personal data continues to flow with the European Economic Area (EEA) post exit. However, there are preparations you can undertake now in readiness for leaving the EU on 29 March 2019. Guidance is available on the ICO website here.

What will change when the UK leaves the EU?

If we leave without a deal, there will be no immediate change in the UK's own data protection standards. This is because the Data Protection Act 2018 will remain in place and the EU Withdrawal Act would incorporate the GDPR into UK law to sit alongside it.

In recognition of the unprecedented degree of alignment between the UK and EU's data protection regimes, the UK would continue to allow the free flow of personal data from the UK to the EEA. This is because data controllers within the EEA, i.e. EU states plus Norway, Iceland and Liechtenstein, are covered by the GDPR.

However, you will need to take action to ensure EEA organisations are able to continue to send you personal data.

Does my organisation need to do anything now?

It is important for all organisations, as a priority, to review whether they would be affected by assessing their data flows. For those that would be affected, early action is strongly advised as changes may take some time to implement.

Inbound personal data flows from the EEA may be affected. We recommend that you identify inbound personal data flows, which are data transfers from any EEA organisation to your organisation.

We would recommend that you contact these EEA organisations to discuss and put in place the relevant appropriate safeguards. Please note that these safeguards can be implemented now.

If your organisation is affected, you should review the technical notice issued by the UK government and ICO guidance now, and encourage organisations in the EEA that you exchange personal data with to do the same.

Organisations should also identify any EU databases, networks or information systems that you currently have access to, and rely on, and consider if you need to develop alternative arrangements to continue receiving the data in a no deal scenario.

What is an adequacy decision?

A transfer of personal data to a 'Third Country' (countries that are not within the EEA) may take place where the European Commission has decided that the third country ensures an adequate level of protection so that a transfer of personal data does not require any specific authorisation.

Will we have an adequacy decision when the UK leaves the EU?

We do not expect the European Commission to have provided the UK with an adequacy decision by 29 March 2019.

Which data flows may be affected when we exit the EU?

Outbound flows of personal data

Outbound personal data flows (from the UK to the EEA) will be able to continue from the UK to the EEA and other adequate countries (countries that have received an adequacy decision) once the UK has left the EU. This is because the UK is putting in place a statutory instrument (SI) that will allow the free flow of personal data from the UK to the EEA.

The US government and the ICO have published guidance for how personal data can continue to flow from the UK to the US under the Privacy Shield in a no deal scenario. UK organisations will continue to be able to transfer personal data to US organisations participating in the Privacy Shield provided those organisations have updated their public commitment to comply with the Privacy Shield to expressly state that those commitments apply to transfers of personal data from the UK.

Rules on transfers of personal data to countries that are currently non-adequate third countries will not change.

Inbound flows of personal data

Inbound personal data flows (from the EEA to UK) **may** be affected. Once the UK has left the EU on 29 March 2019 its status under GDPR is that of a 'Third Country'. The UK will not be considered adequate until the European Commission has undertaken an assessment of our data protection legislation. This means that data controllers and data processors within EEA jurisdictions are restricted from sharing personal data in the absence of an alternative legal basis, such as one of the standard contractual

clauses approved by the European Commission. The European Data Protection Board (EPDB) has issued an information note for commercial and public organisations in EEA countries on what instruments can be used when transferring personal data to the UK.

In the absence of an adequacy decision can we still receive personal data?

If a third country does not have adequacy decisions from the European Commission, EEA organisations can put in place appropriate safeguards so that there is a legal basis to transfer personal data.

What is an appropriate safeguard?

The most common safeguard used to transfer personal data to third countries are standard contractual clauses. You can find out about these, and how to implement them, on the ICO website here.

In some circumstances you may wish to consider using a different appropriate safeguard in Article 46 of the GDPR – for instance, for sharing between public sector bodies you may wish to consider using a legally enforceable contract. In other circumstances you may wish to rely on one of the derogations in Article 49. Information about these can be found on the ICO website here.

How do I use standard contractual clauses?

Standard contractual clauses (SCC) are pre-approved by the European Commission and can be inserted into new, or existing, agreements to provide a legal basis for transferring personal data from the EEA to a non-adequate third country. In a 'no deal' scenario they are expected to be widely relied upon for EEA to UK data transfers.

Further advice, and guidance, on SCCs is available on the ICO website. This includes an interactive tool to help businesses understand and complete SCCs for personal data transfers. Please make sure to check all final products with your own legal team.

How can EEA data processors ensure themselves of adequacy?

Separate guidance about transfers of personal data from processors based in the EEA will be published shortly.

What will happen to the patient records of UK citizens who have been living in the EEA who return to the UK post exit?

General practitioners (GPs) in the UK can request a copy of a patient's medical records from an EEA GP on behalf of their patient.

Are there any Cyber Security issues?

In order to ensure that your data and digital assets are adequately protected it is imperative that your annual Data Security and Protection Toolkit assessment is

completed. This self-audit of compliance with the 10 Data Security Standards is mandatory to complete by the end of March 2019. Completing it early will enable health and adult social care providers to more quickly identify and address any vulnerabilities.

If you identify any data flows, databases or data stored in the EEA which are critical to patient care?

It is imperative that you let NHS England and Improvement know by contacting your regional EU Exit inbox. These inboxes will either be able to provide the appropriate advice or escalate concerns to the EU Exit Co-ordination Centre. Contact details for the regional EU Exit leads are set out below.

If you identify data flows, databases or data stored in the EEA which if withdrawn or disrupted would have a serious impact upon your organisation what should you do?

It is imperative you let NHS England and Improvement know by contacting the regional EU Exit leads as set out below.

What additional assistance will be made available by NHS England and Improvement?

Local teams will support any issues that may arise from EU Exit. Any issues can be escalated to the regional teams as required and where issues impact across the health and care system at a national level these will be escalated to the EU Exit National Co-ordination Centre who will coordinate flows and responses as required.