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

Dawn Monaghan, Head of Data Sharing and Privacy (NHS England), Head of Strategic IG (NHS Digital) and Director Information Governance Alliance, and Keith Willett, EU Exit Strategic Commander and Medical Director for Acute Care & Emergency Preparedness, have written to NHS organisations 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](https://www.england.nhs.uk/publication/eu-exit-personal-data/) as part of the Government’s contingency preparations for a ‘No Deal’ Exit from the European Union (EU).

The guidance sets 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.

The following post details the guidance outlined in the letter and links to the accompanying Q&As that is currently being cascaded out to NHS organisations and other stakeholders.

**Guidance Summary**

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 available here: <https://www.england.nhs.uk/eu-exit/data/>. This guidance explains 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.

Please note that there has been some website content produced on the same subject, available here: <https://www.england.nhs.uk/eu-exit/data/>