Health Research Authority

Data Protection Impact Assessments (DPIAs) and IG standards for Sponsors

RD Forum Non-commercial Sponsor Symposium

9th December 2020

Alastair Nicholson, Health Research Authority

Alex Bailey, MRC Regulatory Support Centre

Health Research Authority

Overview

- Background
- New DPIA Guidance
- New EHRs Guidance
- Next Steps… Sponsor Standards
- MRC and Discussion

Background

- GDPR / DPA 2018
- (UK) GDPR will embed GDPR in UK regs post 31 December 2020
- Purpose is fundamental to interpretation of GDPR
- All Processing has a Controller

Controller

"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."

DPIA

The research Sponsor is the Controller of Personal Data Processed for the purpose of the research. The Participating Organisation is the Processor of the Sponsor for the purpose of the research

Health Research Authority

*“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."*

Data Protection Act 2018 (64(1))

Health Research Authority

"A data protection impact assessment must include the following—

(a) a general description of the envisaged processing operations;

(b) an assessment of the risks to the rights and freedoms of data subjects;

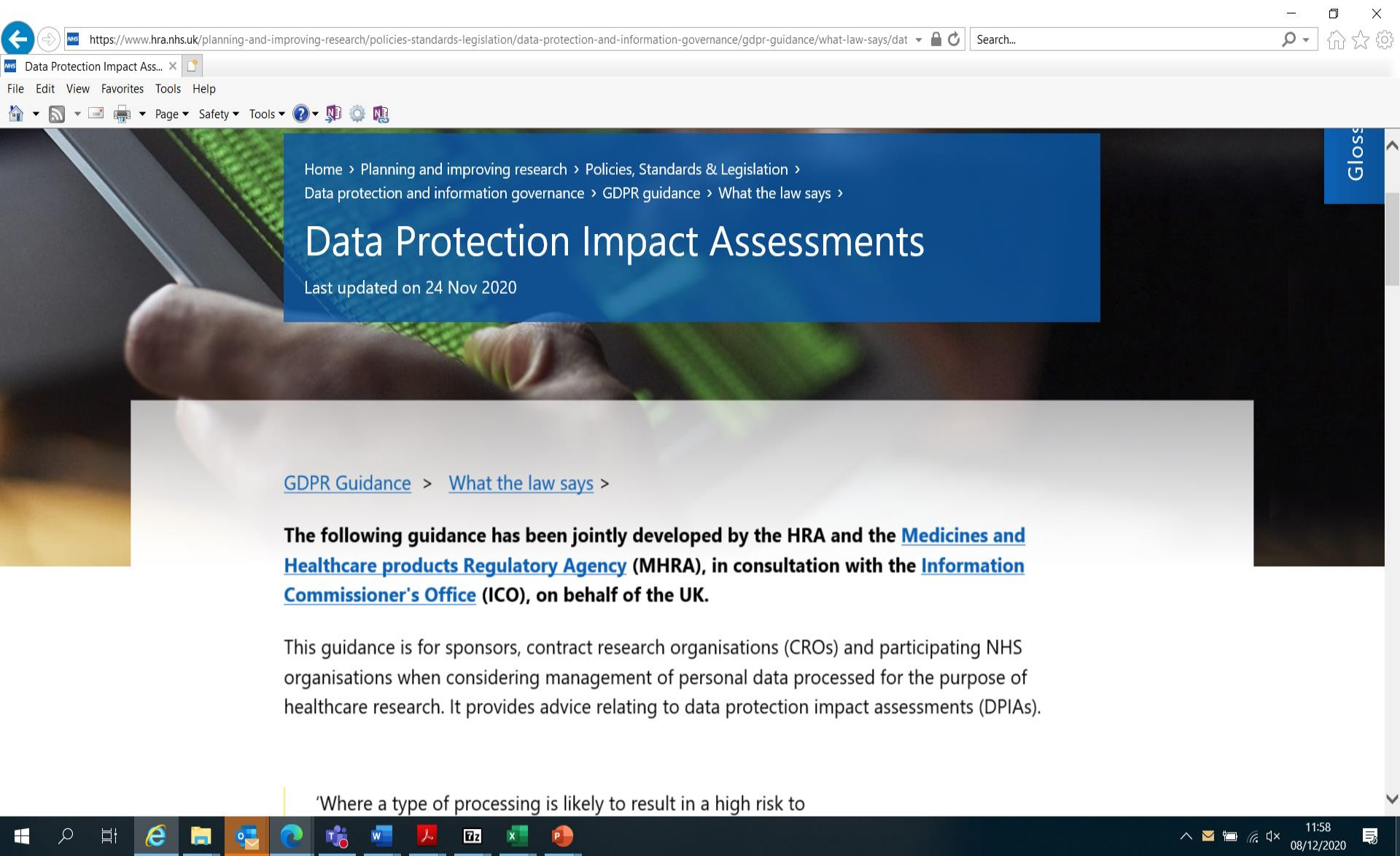
(c) the measures envisaged to address those risks;

(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned."

Data Protection Act 2018 (64(3))

https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/data-privacy-impact-assessments/

NHS Health Research Authority



Summary of Guidance

- Sponsors are responsible for research DPIAs, not sites
- DPIAs should be part of the overall Quality Management System
  - the systems, processes, policies, templates, etc. within which studies are designed are the object of the assessment, not individual studies
- Study specific DPIAs to be considered only when a study falls outside of established IG practice

Summary of Guidance

- Sponsors must exercise due diligence in selecting sites as processors
- NHS sites should ensure that their own processes take account of foreseeable research use and this should be explicitly included in their own DPIAs

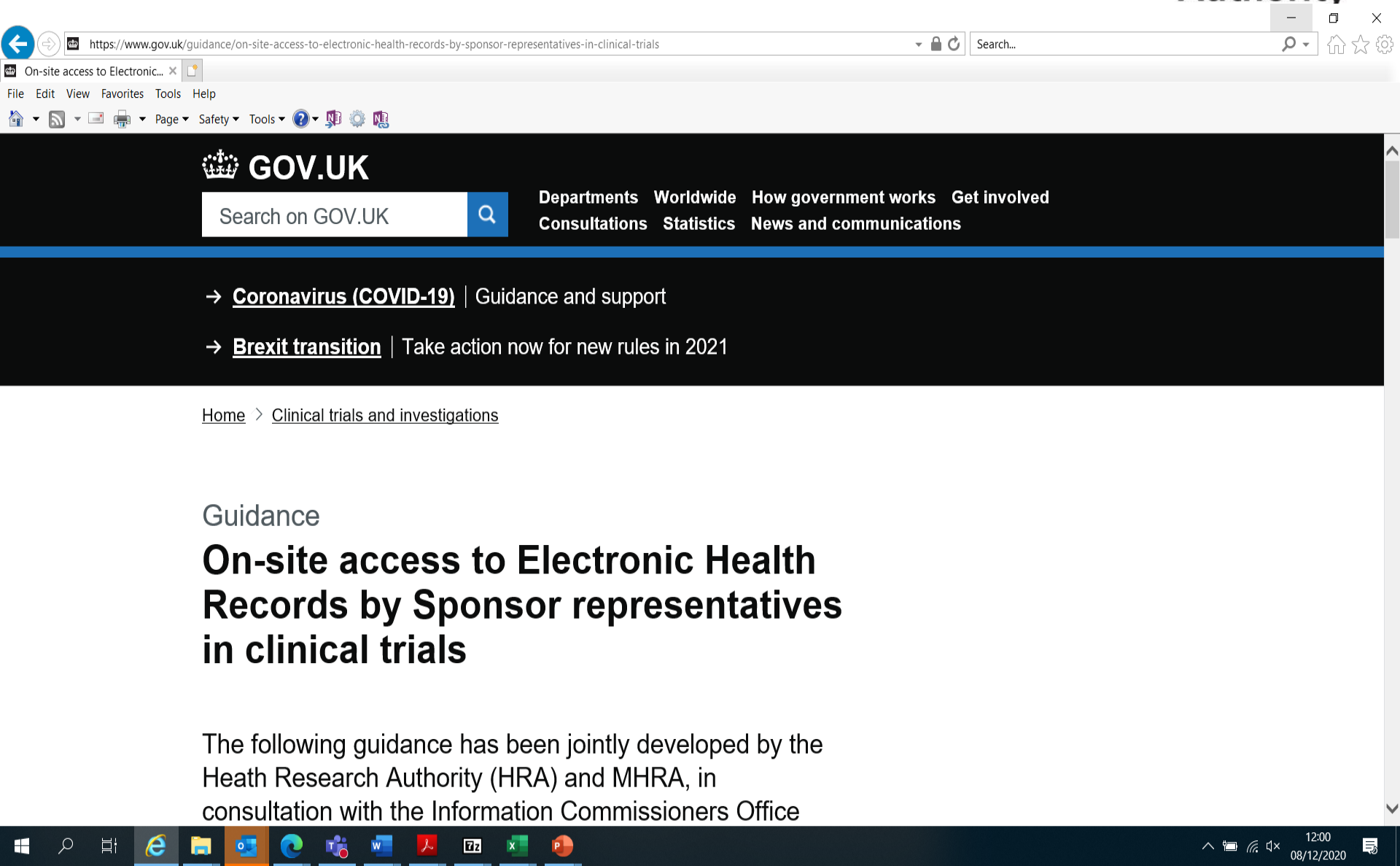
Health Research Authority

For example…..

- Access to EHRs by research sponsor representatives should be set out in DPIAd sponsor processes
- Such access should also be accounted for in the DPIAs of site policies, processes, systems, etc.

https://www.gov.uk/guidance/on-site-access-to-electronic-health-records-by-sponsor-representatives-in-clinical-trials

NHS Health Research Authority



Summary of Guidance

- “Provision of research monitor access to EHRs should be an integral part of organisational level (or EHR level) planning and risk assessment. EHR system design should ensure research monitor access is limited to only the records of clinical trial participants and that this access is auditable”
- If not, this needs to be addressed in next system update

Summary of Guidance

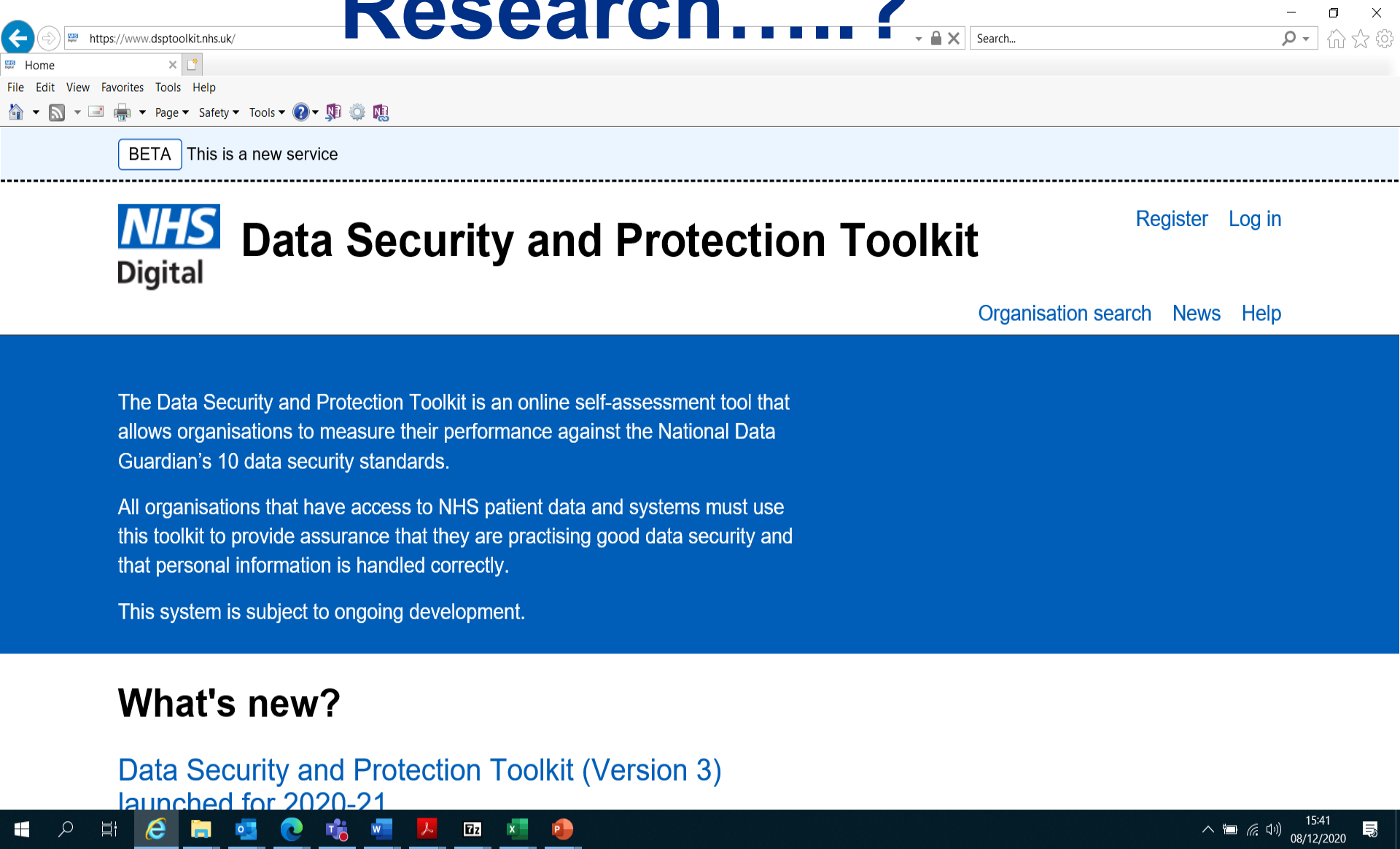
- Short term risk assessed measures should be put in place – these should ensure access to EHR and **NOT** resort to print-outs
- Provision of access on basis of standard agreement terms – i.e. **NO** additional NDAs, etc.
- Monitor accountability via employment contracts
- Training for Monitors, including actions in case of inadvertent breach

Next Steps

- Resilience programme / MHRA stakeholder group on GCP guidance for EHR
- Iteration of UK Study Wide Review Criteria
- Call for stakeholder engagement on major revision of UK SW
- Sponsor standards for designing and managing IG compliant studies

A DSPT / DPIA for Research…..?

Health Research Authority



MRC and Discussion

Health Research Authority

alastair.nicholson@hra.nhs.uk

https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/guidance-health-and-social-care-researchers-end-transition-period/

NHS Health Research Authority

Use of Data at the end of the transition period

The latest information on data transfer and legal requirements at the end of the transition period is being published by the ICO.

The guidance says:

> 'The UK government has stated that, after the end of the transition period, transfers of data from the UK to the EEA will be permitted. It says it will keep this under review.
>
> The UK is England, Scotland, Wales, and Northern Ireland. It does not include Crown dependencies or UK overseas territories, including Gibraltar. The UK government will allow transfers to Gibraltar to continue.
>
> If your restricted transfer is not to the EEA, you should already have considered how to comply with the GDPR. You will continue to be able to rely on the same mechanisms.'

For UK Sponsors of a study with participants in the EEA, DHSC End of Transition Period Data Preparedness Guidance is available on request by emailing: queries@hra.nhs.uk

Glossary