The Life Sciences Lawyer

Issue 1 2021

GLOBAL REACH, LOCAL KNOWLEDGE

www.lslawmag.com

A Portuguese and European perspective on telemedicine and e-health

Ricardo Costa Macedo and Diana Mâncio da Costa, of Caiado Guerreiro, Sociedade de Advogados, discuss the needed reinvention of medical care and how it is redefining the relationship between healthcare services providers and patients.

CTC Legal Media

Health data in the UK: What's next for 2021?

Jaspreet Takhar, Senior Associate at Baker McKenzie, suggests what Brexit and NHS information governance will mean for data transfers, sharing, and use in 2021.

2020 was a big year for health data in the UK. In the year of Brexit and COVID-19, information governance was key. So what does 2021 have in store? We anticipate a final decision on the status of transfers of personal data from the EEA to the UK, post-Brexit. Data sharing collaborations between the private and public sector will continue to be a hot topic. Finally, NHSX will continue to enhance NHS information governance requirements, including the National Data Opt-Out and records management guidance.

Health data in 2020

2020 saw some key developments for health data in the UK. With the Brexit transition period now over, organisations must comply with the GDPR as it is incorporated into national law (UK GDPR). Towards the end of 2020, NHSX also launched a brand new information governance portal, providing a 'one-stop shop' for NHS policies and guidance.[1] NHS supplemental laws and guidance have traditionally been difficult to navigate, so this is welcome news for NHS suppliers and collaborators. Finally, there was a renewed focus on medical confidentiality, and the National Data Guardian made some updates to the Caldicott Principles.

Jaspreet Takhar

> **Data sharing between the private and public sector will be a hot topic.**

5 topics on the horizon for 2021

1. **Partnerships between the NHS and the private sector**

We have seen an explosion in the number of collaborations between the NHS and the private sector in recent years. The private sector is increasingly accessing and using datasets from various NHS organisations to develop data-driven healthcare technology. These partnerships continue to come under the spot-light of media and government. Commentators are scrutinising compliance with data privacy and the common law duty of confidentiality. NHS organisations are increasingly asking, what is in it for the public sector in these deals?

2020 saw NHSX publish a Data Sharing Agreement (DSA) template.[2] The DSA template is a useful tool for companies collaborating with NHS organisations to access and use data (as well as for a host of other purposes). The DSA encourages the relevant NHS organisation and its counter-party to consider key risks related to data privacy and medical confidentiality. Crucially, the parties will need to set out the basis on which personal data (and any special categories of data, such as health data) are shared under both the GDPR and the common law duty of confidentiality.

These partnerships will continue to be an area of focus for the NHS in 2021. We expect organisations such as NHSX will continue to issue guidance focussing on demonstrating compliance and value for the NHS in these partnerships.

2. **Anonymisation and the (messy) intersection of data privacy and the common law duty of confidentiality**

NHSX's Health and Care Information Governance Panel (Panel) informs NHS priorities for new information governance guidance. In their last meeting of 2020, the Panel highlighted pseudonymisation as an area of focus.[3]

Résumé

Jaspreet Takhar, Senior Associate

Jaspreet advises market-leading tech and healthcare companies on issues at the cutting-edge of digital health. She focuses on the development and regulation of healthcare technology. This includes assessing how digital health solutions can comply with the legal framework for data privacy, medical research and medical devices / pharmaceuticals. Jaspreet also advises clients on accessing and using patient data, innovative collaborations with hospitals, and the use and regulation of AI in the healthcare space.

Once data is truly anonymised, it will not fall within the scope of the GDPR and it becomes easier to use. However, anonymisation under the GDPR is a high bar and very difficult to achieve in practice. It involves removing personal identifiers, both direct and indirect, that may lead to an individual being identified. This is more stringent than the traditional understanding of 'anonymisation' under the common law duty of confidentiality as it applies in the healthcare sector.

Often, data considered 'anonymised' for confidentiality purposes is actually 'pseudonymised' data for GDPR purposes. Pseudonymised data may include data where key identifiers have been removed and the data can no longer be attributed to a specific individual without the use of additional information (and such additional information is kept separately and subject to certain technical and organisational measures to ensure non-attribution to an individual). The key takeaway is that pseudonymised data is still personal data subject to the GDPR.

The Panel appears to have picked up on this discrepancy on the thresholds for anonymisation under the GDPR and the common law duty of confidentiality. The minutes[4] of the last Panel meeting identifies *"the issue around how the health and care sector would handle pseudonymised data - if it should be treated as confidential patient information and what safeguards are required to ensure pseudonymised data is not re-identified."*[5] A dedicated working group is being set up to discuss this, so watch this space for further developments.

3. National data opt-out deadline: 31 March 2021

The national data opt-out[6] is a service allowing NHS patients to opt out of their confidential patient information being used for research and planning. The information includes that collected in the course of publicly funded, commissioned or coordinated health and adult social care, as well as private care given in NHS settings. The national data opt-out does not apply where data is shared for a patient's care.

All health and care organisations that process health and social care information as a controller must be compliant with the national opt-out policy by 31 March 2021.

The original deadline had been extended to enable health and care organisations to focus their resources on the COVID-19 outbreak. In-scope organisations must ensure there are systems in place to facilitate a patient's opt-out and processes to ensure that patient's data is not used for research and planning purposes.

> **"Once data is truly anonymized, it will not fall within the scope of the GDPR."**

4. Brexit and EEA to UK transfers of personal data

EEA to UK data transfers: On Christmas Eve the UK and the EU concluded a Trade and Cooperation Agreement (Agreement) in principle, and there was one Christmas present for data protection lawyers: the transfer of personal data from the EEA to the UK may continue without safeguards (e.g. standard contractual clauses) from 1 January 2021 for a period of four months. This period will be automatically extended by a further two months if neither the UK nor the EU objects. This is on the condition that the UK continues to apply the UK GDPR. The period will end earlier if the European Commission adopts an adequacy decision in relation to the UK.

UK to EEA data transfers: The Agreement did not address transfers of personal data from the UK to the EEA, but these transfers can also continue without safeguards after the transition period because the UK has already designated EEA member states as providing an adequate level of protection of personal data for the purposes of the UK GDPR. This designation can be withdrawn at any time.

5. New Records Management Code of Practice

The Records Management Code of Practice (2016) (Code) sets out what people working with or in NHS organisations in England must do to correctly manage records. The Code focuses on how long records should be retained by an organisation in possession of NHS data. It is based on the legal requirements and professional best practice published by the Information Governance Alliance in 2016.

Despite only being a few years old, the Code is already out-of-date (it pre-dates the GDPR). A consultation for a new Records Management Code of Practice 2020 recently concluded, so a new version is in the works.[8] The revised version of the code will be published once NHSX have analysed the responses and updated the code. The 2016 version is still valid until the new code has been finalised.

1 https://www.nhsx.nhs.uk/information-governance/guidance/

2 https://www.nhsx.nhs.uk/information-governance/guidance/data-sharing-agreement-template/?utm_source=twitter&utm_medium=social&utm_campaign=ig_staff

3 https://www.nhsx.nhs.uk/information-governance/health-and-care-information-governance-panel/minutes/2020-09-15/

4 https://www.nhsx.nhs.uk/information-governance/health-and-care-information-governance-panel/minutes/2020-09-15/

5 https://www.nhsx.nhs.uk/information-governance/health-and-care-information-governance-panel/minutes/2020-09-15/

6 https://digital.nhs.uk/services/national-data-opt-out

7 https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-857-F1-EN-ANNEX-1-PART-1.PDF

8 https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/

Contact

Baker McKenzie
100 New Bridge Street, London EC4V 6JA, United Kingdom
Tel: +44 20 7919 1000
Jaspreet.Takhar@bakermckenzie.com
www.bakermckenzie.com/en