Shared Insights

Data and Information Governance Issues

Charlotte Harpin, Partner,
Browne Jacobson

Matthew Alderton, Partner,
Browne Jacobson

6 June 2023

Browne Jacobson

Introduction

Charlotte Harpin and Matthew Alderton chaired a session on data and information governance issues which covered:

- Legal update and the steps your organisation needs to take to prepare for and implement the new legislative changes.
- What to do when the worst happens: dealing with ICO review, reprimands, data breaches and damages claims.
- Best practice and common pitfalls when dealing with Subject Access Requests (SARS).
- Top tips for dealing with WhatsApp, Social Media and Covert filming. What should you do if a patient or relative is commenting negatively on social media or sharing photos or comments about staff or other patients? What if a patient wants to film an operation, clinic appointment or even labour and delivery? What is the guidance for dealing with covert filming? And what key messages should you share with staff about WhatsApp, text messaging and their own social media use?
- Regulatory developments in relation to the use of AI and other new technologies within the NHS

Legal Update – What do you need to start thinking about?

- Data Protection Bill – key changes:
  - Easier processing for legitimate interests and research purposes
  - DPIAs for high risk processing only
  - Change to DPOs
- Online Safety Bill:
  - Additional protections for vulnerable
  - Offences relating to harmful content

Charlotte Harpin
Partner
+44 (0)330 045 2405
charlotte.harpin@brownejacobson.com

Matthew Alderton
Partner
+44 (0)330 045 2747
matthew.alderton@brownejacobson.com

Recent case law

&

ICO review and reprimands

Recent case law

- Prismall v Google/DeepMind – primarily about class actions but has some helpful paragraphs on health data and when the use or misuse of data would be unlawful. The Court found that not every piece of medical information is inherently private. There were important findings around sensitivity of medical records.
- EU caselaw:
  - TU and RE v Google LLC (Case C-460/20) - what you need to consider for erasure and accuracy disputes. See also Dixon v North Bristol NHS Trust [2022] EWHC 3127 (KB)) about why it is important to maintain original documents.
  - OT v Vyriausioji tarnybinės etikos komisija (Case C-184/20) – data protection rights are not absolute
  - Case C-300/21 UI v Österreichische Post AG (EU:C:2022:756) – damages do not automatically follow a contravention of the GDPR (see also the UK cases of Johnson v Eastlight; Rolfe v Vizards; Stadler v Currys)

Information Commissioner's Office (ICO) review and reprimands

- ICO resources – helpful first step if unsure
  - SARs Q&A for employers | ICO
- Approach of the ICO
- How the ICO enforces (Nov. 2022). A different approach is being trialled with reprimands rather than fines being issued to public bodies.
- If the breach is a cyber incident, don't forget the potential for NCSC reporting in addition to the ICO
  - Data security incident trends | ICO
- Notable enforcement action taken by the ICO in the last year
  - Reprimands – reputational damage and wider regulatory impact?
    - Failure to ensure appropriate safeguards in place to mitigate against risks associated with administrative/ human error breaches
    - Failure to meet statutory response periods for SARs [e.g. only 260 of 511 in time in 1 year]
    - Inadvertent release of untested development code into a live system
    - Records loss following software termination
  - Fines
    - E.g. against TikTok

Data breaches and damages claims

&

Subject Access Requests

Data breaches and damages claims

Data breaches continue to make the news

- Common risk areas remain:
  - Human error (often combined with inappropriate administrative practices/workarounds)
  - Cyber attacks / weaknesses [direct/third party – see e.g. Capita]
- Highlights of recent case law on damages claims and the court view on class actions for data protection matters
  - Lloyd v Google [2021] UK SC 50
  - SMO v TikTok
  - Prismall v Google/Deep Mind

Subject Access Requests (SARS)

The ICO has published new guidance for employers

SARs Q&A for employers | ICO

Some common issues we come across:

1. Extending time for compliance
2. Manifestly excessive SARs
3. Mixed personal data
4. Duty of confidentiality
5. Clinical input
6. Requests from the police
7. Children's personal data
8. Deceased patient records

We were delighted to be joined by Fiona Hobday, Interim Head of Information Governance at United Lincolnshire Hospitals, who shared her experiences from a number of public sector organisations, of dealing with SARs, which have increased in volume and complexity. The increased use of multiple digital systems and implementation of new technology has added to this. Information within the NHS is becoming more fragmented. It is important to identify complex SARs as early as possible and explain to the individual that it may take longer to help manage expectations.

Social Media

&

The use of AI and other technologies

Social media

- Use of social media by patients. We deal with cases where the content can be distressing or amount to harassment and have worked with social media companies to get content removed but it isn't a quick process. Hopefully there will be more tools available to us under the Online Harm Bill.
- Covert filming. There are limits on what you can do but set expectations within the organisation. Ask patients to be open if they are filming.
- Use of social media by staff – WhatsApp messages form part of the decision making record and can be disclosable. It is important that staff are aware of this.
- Misuse of social media can amount to professional misconduct and result in regulatory action
- Ensure you have a Social Media Policy and that staff are aware of it. This is something we can help with.

The use of AI and other technologies

- Lots of buzz and plenty of potential to help deliver improvements to patient care/patient experience.
- Essentially the same legal framework as for any other technology in a medical setting but you do need to be aware of the regulatory framework that applies to medical devices - Medical devices: software applications (apps) - GOV.UK (www.gov.uk)
- If medical devices are being manufactured in-house, see In-house manufacture of medical devices in Great Britain - GOV.UK (www.gov.uk)
- Keep informed about the as well as the MHRA-led "Roadmap" for AI Software and AI as a Medical Device Change Programme - Roadmap - GOV.UK (www.gov.uk)
- Note the adverse incident reporting requirements for software as a medical device Guidance for manufacturers on reporting adverse incidents involving Software as a Medical Device under the vigilance system - GOV.UK (www.gov.uk)
- Apps – Vigilance requirements (Field Safety Notices and End-of-Life notification requirements)
- Use tools like DPIA; EQIA etc. to help assess risks and implement appropriate mitigations.

Discussion

&

How we can help

Discussion

- A number of issues were discussed, including
- Redaction
- The need for clinical review by clinicians – have a threshold for this as it is not necessary (or proportionate) in every case
- Where it is considered that disclosure will harm a patient, can this be minimised by sitting down with patients and discussing the distressing aspects with them.
- Describing documents by category and seeking clarification of vague requests
- Whether records relating to certain areas of medicine such as mental health and fertility are automatically sensitive. This is case specific and depends on how much information is already in the public domain, for example where the person has already shared information on social media.
- How “serious harm” is quantified. Push back and ask for information about how the breach caused damage. Consider what information was disclosed and how was the breach mitigated.

How we can help

- Helping you update your policies and procedures to take into account legislative changes
- Advising you on handling data breaches, including protecting against breaches, breach management and recovery
- Helping you to set up processes, policies and templates for handling complex SARs
- Advising on international opportunities in relation to data (including AI and App development and deployment), and the associated regulatory issues arising
- Supporting the development and implementation of digital strategies at an organisation/ICS/multi-ICS level
- Acting as a connector in the data sector and facilitating peer-learning/expert input
- Keep a look out for the formal launch of our data focussed programme in the autumn and please do send across any topic suggestions or let us know if you’d like to participate (thanks to those who have already been in touch).

Contact us

Lorna Hardman
Partner

+44 (0)115 976 6228
lorna.hardman
@brownejacobson.com

Simon Tait
Partner

+44 (0)115 976 6559
simon.tait
@brownejacobson.com

Damian Whitlam
Partner

+44 (0)3300452332
damian.whitlam
@brownejacobson.com

Nicola Evans
Partner

+44 (0)330 045 2962
nicola.evans
@brownejacobson.com

Charlotte Harpin
Partner

+44 (0)330 045 2405
charlotte.harpin
@brownejacobson.com

Matthew Alderton
Partner

+44 (0)330 045 2747
matthew.alderton
@brownejacobson.com

brownejacobson.com
+44 (0)370 270 6000

Please note:
The information contained in this document is correct as of the original date of publication.
The information and opinions expressed in this document are no substitute for full legal advice, it is for guidance only.

Browne Jacobson