Guidance for General Practices: Data Use and Access Act 2025 (DUAA)

An update by the Information Commissioner's Office (ICO) on 19 June 2025 (focusing on what the revised legislation means for regulated organisations) has been used to inform this guidance document for LMCs.
The ICO update can be found HERE.

Overview

The DUAA updates existing laws on digital information, data protection and data use across public and private sectors. It aims to:

- promote innovation, research and digital development
- simplify data protection requirements
- maintain patient rights and confidentiality

Changes apply gradually from June 2025 to June 2026 and mainly streamline current processes.

What laws does the DUAA change?

The DUAA amends, but does not replace:

- UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018 (DPA)
- Privacy and Electronic Communications Regulations (PECR)

General practice information governance (IG) policies remain in place, but some processes become clearer and easier.

Key Points for General Practice

Research and statistics using patient data – broader definitions and easier consent

The DUAA clarifies when you can use personal information for scientific research (including commercial research). Patients can now give *broad consent* to an area of scientific research.

GP practices involved in academic or NHS research programmes can:

- rely on broad consent if aligned with ethical standards
- use data for scientific, public health or statistical research with appropriate safeguards

---

Privacy notices – reduced obligation in some research uses

Personal information can be reused for scientific research without providing a privacy notice if that would involve a disproportionate effort. Patient rights must be protected in other ways, and practices must still need to make information publicly available by publishing a notice on the practice website.

This is useful for retrospective studies and public health research using legacy patient data.

Automated decision-making – wider allowance but still with safeguards

The DUAA expands the lawful bases (full range of reasons) that you can rely on when you use people's personal information to make significant automated decisions about them.

GP practices using automated systems (triage chatbots, decision-support tools, online booking algorithms, etc.) must continue to provide human review options and "special category data" (including health data) still has extra restrictions.

Changes to patient messaging and marketing

Cookies and website analytics
Some performance and statistical cookies may be set without explicit patient consent.

Email contact rules
Practices sending recall or screening emails can continue to rely on existing consent or public task basis, not the charity rule (which now allows a soft opt-in for email marketing). A charity that has collected a person's personal information because they've supported, or expressed an interest in, their work, can send them direct marketing emails, unless they ask it not to.

Breach notifications
Time to notify the ICO of a Privacy and Electronic Communications Regulations (PECR) breach is now increased from 24 to 72 hours (aligned with GDPR).

New recognised legitimate interests lawful basis option under UK GDPR – easier justification for processing personal data in safeguarding, emergencies, crime and public interest

When personal information is used for certain **recognised legitimate interests**, there will no longer be a need to balance the impact on the people whose personal information you use against the benefits arising from that use. This applies to specific situations such as safeguarding, responding to emergencies, crime prevention, detection and prosecution, and national and public security.

Disclosures that help other organisations perform their public tasks

You are allowed to give personal information to organisations such as the police without having to decide whether that organisation needs the information to perform its public tasks or functions, providing that the organisation has confirmed it needs the information to carry out its public task.

Subject Access Requests (SARs) – more flexibility and clarity

Legal changes now provide clarity that practices only have to make **reasonable and proportionate searches** when someone asks for access to their personal information.

- Practices can "stop the clock" to ask for clarification if a SAR is unclear.
- Time limits start once practices receive the request, ID information (if asked for), or any fee for manifestly unfounded / excessive requests.

Data protection complaints handling – simple patient route required

Organisations must provide a simple route for people who want to make complaints about how their personal information is used (such as an electronic complaint form). Practices must:

- acknowledge complaints within 30 days
- keep patients updated
- respond fully "without undue delay".

Regulatory change – ICO becomes the Information Commission

The Information Commissioner's Office (ICO) becomes the **Information Commission** by 2027.

Powers increase (interviews, higher fines, technical reports).

Enhanced powers for the Secretary of State

The DUAA amends the law so that **information standards** under the Health and Social Care Act 2012 may now include information technology (IT) and IT services used in health and adult social care.

The DUAA embeds into law the requirement that health-care IT systems meet common technical and data-handling standards.

- The Secretary of State (and in some cases NHS bodies) will have the power to publish, set or adopt those standards.
- The Secretary of State can also add further safeguards around using personal data for research.

Practice IT systems may need to meet new technical / data-handling standards or use specific IT services, but until the standards are published and enacted, it is unclear how immediate the impact will be.

What has not changed?

- Clinical confidentiality remains unchanged.
- NHS Data Security and Protection Toolkit (DSPT) still applies.
- Health data remains protected as special category data.
- DUAA changes do not override NHS data sharing or common law confidentiality.

ICO Support

The ICO will:

- update guidance during 2025–26 as changes come into effect (practices can sign up to ICO newsletters and e-shots to be notified of this)
- provide detailed information for DPOs and IG leads
- publish codes of practice for EdTech and AI (including impact assessments and consultation with relevant organisations).