October 28, 2026

European Data Protection Board

Submitted via web to the EDPB

RE: Public Consultation on the Guidelines 02/2026 on Anonymisation

To the European Data Protection Board:

We appreciate the opportunity to provide feedback on the European Data Protection Board's (EDPB) draft Guidelines 02/2026 on Anonymisation (the "Guidelines").

Epic is a global healthcare technology company working with healthcare organisations in more than 15 countries worldwide, including multiple across the European Economic Area. Our integrated software suite helps healthcare provider organisations across the European Economic Area manage over 20,000,000 patient visits each year. We provide decision support and research capabilities that promote the delivery of high-quality clinical care. Clinicians across the world can use our software to leverage analyses of pseudonymised and anonymised patient data to treat patients with ultra-rare diseases, better predict hospital length of stay, and provide better medication management for patients with complex co-morbid chronic illness.

As an electronic health record (EHR) software developer, our comments about the Guidelines focus on the technical mechanisms and criteria the Guidelines set to achieve effective anonymisation. We seek to balance privacy with useful data tooling. Preserving the rights, protections, and privacy of all persons is paramount and, in our experience, can be achieved while also providing a clear, actionable anonymisation strategy.

We would welcome the chance to discuss our recommendations further as the EDPB finalises the Guidelines. Thank you for your consideration.

Sincerely,

Katherine Hou
Public Policy

Amanda Reese
Privacy Counsel

Specific Comments

The three criteria challenge health data usability

Epic supports the goals the EDPB has articulated in the Guidelines, including ensuring that personal and anonymous data is used in a way that is lawful, beneficial, and safe. However, we are concerned that the proposed criteria will undermine the achievement of the Guidelines' desired outcomes and will diminish the ability to make health data useful at individual healthcare organisations and within the European Health Data Space.

Health data is most useful when it is accurate, complete, and detailed. Individual records may be linked to extensive social, demographic, and clinical information, some or all of which may flow into datasets built from the aggregation of such records. Analyses of health datasets can inform meaningful individual and population care, especially when the comprehensive range of attributes are considered in the analysis. However, the Guidelines' three criteria for anonymisation set a standard, which, if met, would render the resulting data minimally useful when promoting health at the individual or population levels.

Health datasets can include longitudinal extracts of patients' entire health journeys. The breadth of this information, when analysed over a population, is particularly valuable for investigating how certain treatments might produce better patient outcomes than others. These decisions are most accurate when informed by analyses of large datasets of social and clinical data points that help isolate a treatment's effects from other determinants of health, meaning that a robust dataset is more beneficial for patient care. The breadth of data points required to inform a conclusive investigation makes it likely that included records will be unique. Since No Record Isolation requires that the data does not contain unique combinations of attributes relating to single individuals, a dataset that fulfils the No Record Isolation criterion would not allow for meaningful population health intervention. Limiting unique attribute value combinations limits the ability to track relevant outcomes and leads to weaker, less insightful conclusions.

The Guidelines' No Linkage criterion also creates practical limitations for managing patients' health. Patients routinely seek clinical care from multiple healthcare providers who provide care as part of a network. Any dataset generated by providers in the network would likely cover overlapping populations. Since healthcare encounters often cover the same foundational topics, data attributes like sex, presentation of illness, and past medical history could hold the same information for an individual at multiple providers. These data attributes may be the exact categories helpful for initiating proactive public health campaigns or analysing seasonal health trends at provider organisations. However, No Linkage holds that the ability to use those attributes to link records between datasets violates anonymity. Fulfilling the No Linkage criterion would complicate any meaningful analysis of health data if it leads providers to remove useful data attributes from their datasets.

The Guidelines' No Inference criterion will also restrict healthcare providers' ability to use datasets for public health monitoring. The Guidelines' Example 19 describes a scenario where a health dataset that includes diagnosis and demographic information violates the No Inference criterion since it could lead to specific and meaningful inferences when combined with other data about an individual. As described previously, diagnosis and demographic data are often the most relevant attributes used to inform public health campaigns. Fulfilling No Inference by removing these attributes from a dataset would leave the data less useful.

As currently drafted, the Guidelines' three criteria for anonymisation could negatively impact healthcare providers and hospitals by hindering them from leveraging innovative, data-driven, privacy-protecting analyses that could improve the quality of care they provide.

Define a probabilistic, risk-based standard for anonymisation that supports data usability

To improve patient care by facilitating the adoption of data-informed technologies, we recommend revising the Guidelines to provide a defined methodology for anonymisation and a clear evidentiary standard for achieving anonymisation.

For example, while operating under a different regulatory scheme, the Information and Privacy Commissioner for the Canadian province of Ontario offers practical guidelines on steps organisations can take to perform sufficient de-identification and evaluate the risk of re-identification of data subjects represented within a dataset.[1] The Ontario De-identification Guidelines for Structured Data define anonymity by disclosure type, share calculable equations for the risk of re-identification, and provide reference re-identification probability thresholds tied to impact severity. Risk is scaled by probability of re-identification and potential harm, and evaluation is not absolute. To support organisational implementation of de-identification practices, the Ontario Guidelines also describe a 12-step governance process and provide practical checklists for documenting compliance.

The clarity in scope and practical guidance creates a framework for how organisations can safely de-identify data and use it in their operations in compliance with Ontario's privacy laws, which facilitates anonymised data that is useful and protected. We recommend the EDPB revise the Guidelines to provide a clearer, risk-based framework that does not rely on the three criteria provided (No Record Isolation, No Linkage, and No Inference).

Increase clarity to align with established precedent

We also recommend revising the Guidelines to include specific implementation steps to align with existing approaches to anonymisation in European case law and Commission decisions. Currently, the Guidelines' contextual approach, described in Paragraph 47 as a differentiated assessment based on different perspectives, lacks specificity, and the simplified approach, described in Paragraph 48 as a method that voluntarily overestimates risk, may conflict with existing case law.

The contextual approach will be difficult to implement due to lack of clarity on steps and an unbounded number of potential entities to consider. In a previous decision, the Commission has given affected entities a concrete list of technical and contractual measures to take to ensure adequate anonymisation under the scope of the EU Digital Markets Act.[2] The current Guidelines do not provide specific action items and will lead to execution differences.

For example, in Example 22 in Section 3.5.2, a research institute uses the contextual approach to evaluate the anonymity of their research data, but the Guidelines present no concrete measures to rate the validity of their approach, and it is possible a violation could still be contrived. The institute makes assumptions about relevant entities that might be familiar with the subjects' personal lives, and assumptions about what groups might be able to access the data in the event of a data leak – in light of the context in which the dataset will be accessed and used. They make conclusions based on the specific context and their own subjective reasoning. But without a clear standard for identifying relevant entities or a definition for the likelihood of linkage, different organisations are certain to reach different conclusions; alternatively, organisations may not attempt to rely on the contextual approach at all. Falling back on the simplified approach may become a default option for organisations who lack clarity on executing the contextual approach, yet using the simplified approach will create greater challenges with regard to using the resulting anonymised data.

The simplified approach may lead to inappropriate conclusions that are inconsistent with existing case law. In a previous case, the Court of Justice of the European Union ruled that pseudonymisation is sufficient to prevent identification for certain recipients of a dataset. Even if some controllers could obtain additional information that renders pseudonymised data to be identifiable personal data, that data should not be considered personal in all cases and for every person.[3] Yet the broad strokes used in the simplified method

---

[1] *See* De-identification Guidelines for Structured Data, Updated and Expanded, Information and Privacy Commissioner of Ontario (October 2025); https://www.ipc.on.ca/en/resources/de-identification-guidelines-structured-data.

[2] *SP – Alphabet – Article 6(11)* (Case DMA.100209), Commission Decision of July 16, 2026, 2026 O.J. (C/2026/4443), *available a*t https://competition-cases.ec.europa.eu/cases/DMA.100209

[3] C-413/23 P, European Data Protection Supervisor (EDPS) v. Single Resolution Board (SRB),

conclude that data is not anonymous if even some controllers are able to render anonymous data to be personal. The Guidelines accept that overestimates of risk that exceed the legal standard are probable under the simplified approach, but a higher rate of inappropriately concluding that pseudonymised data is actually identifiable will hinder the usefulness of health data for healthcare provider organisations. Revising the Guidelines to instruct organisations on anonymisation in alignment with existing case law and Commission decisions will support more consistent determinations regarding the level of anonymity in datasets.

2025 ECLI:EU:C:2025:645 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62023CJ0413