SUBJECT

Secondary use of health data recorded for clinical care purposes in non-profit public retrospective research: the case for a proportionality-based safeguard regime accessible to non-profit, unfunded NHS and underfunded academic investigators

COMMENT 1

Reference: §§ 40-50 (Broad and Dynamic Consent) and §§ 53-55 (Consent under ethical/legal requirements vs. GDPR legal basis)

Issue: The Guidelines do not adequately distinguish between commercial and non-profit public research in terms of the operational burden of consent management

The Guidelines, while providing valuable clarity on broad and dynamic consent, apply a uniform framework regardless of whether research is conducted by commercial sponsors with dedicated funding or by non-profit public institutions operating without research budgets.

In practice, for a non-profit NHS investigator conducting a retrospective observational study on i.e. 10,000 patients over a 5-year follow-up period —analytically feasible with freely available machine-learning tools, but lacking external funding or dedicated data management infrastructure — the operational cost of:

- individually contacting 10,000 patients,
- managing broad consent withdrawals,
- maintaining a dynamic consent platform,
- setting up the privacy dashboard recommended at § 80,

represents an **absolute barrier to research**, not a proportionate compliance measure.

This situation is structurally different from a commercial sponsor who can budget consent management as a line item in a clinical trial. The Guidelines do not acknowledge this asymmetry.

Concern: By treating all research controllers identically, the Guidelines implicitly favours well-funded commercial research over underfunded non-profit public research, producing a result that is contrary to the GDPR's stated objective of supporting scientific research as a societal good (Recital 159) and to the EU's commitment to a European Research Area (Art. 179 TFEU).

Suggested amendment to § 41 / § 48:

Example of an explicit guidance clarifying that:

"Where a controller is a non-profit public institution conducting research exclusively in the public interest, without commercial funding, and where obtaining individual consent or managing a dynamic consent platform would require resources that render the research financially impossible, the absence of a consent-based legal basis should not be considered a shortcoming, provided the controller relies on an appropriate alternative legal basis under Art. 6(1)(e) or (f) GDPR, has obtained a favorable opinion from the competent Ethics Committee, and has adopted proportionate safeguards pursuant to Art. 89(1) GDPR."

COMMENT 2

Reference: § 53-55 (Distinction between ethical consent and GDPR legal basis) and § 100 (Disproportionate effort)

Issue: required individual informed consent even when GDPR conditions for exemption are met — the Guidelines should provide clearer guidance to bridge this gap

The Guidelines correctly establish at §§ 53-55 that informed consent required by ethical or legal standards is legally distinct from consent as a GDPR legal basis. This is a crucial clarification.

However, in practice — including the specific Italian regulatory context — Ethics Committees often require individual informed consent from patients as a **condition of ethical approval**, even in circumstances where:

- the GDPR exemption for disproportionate effort (Art. 14(5)(b)) would apply,
- the national law (in Italy: Art. 110, D.lgs. 196/2003 as amended by L. 56/2024) explicitly permits research without consent following Ethics Committee approval,
- the research is retrospective, observational, on pseudonymised data, with no intervention on patients.

This creates a **regulatory paradox**: the GDPR and national implementing law permit the research without consent; yet the Ethics Committee — which is the gatekeeper to the very approval that the law requires — demands consent anyway, thereby re-introducing through an ethical requirement the very burden that the legal reform was designed to remove.

The issue is scientifically severe especially for **deceased patients**, where fulfillment of ethical and GDPR duties is practically impossible but health data are extremely useful for epidemiological and/or public health analysis (see comment 5).

The result is that the reform of Art. 110 of the Italian Privacy Code (May 2024), which eliminated the need for prior Garante consultation specifically to ease retrospective research, is being de facto neutralised by Ethics Committee practice.

Suggested amendment — addition to § 55 or new § 55-bis:

As example, include explicit guidance to the effect that:

"Where national law explicitly permits the processing of health data for scientific research without individual consent — on the basis of a favorable Ethics Committee opinion and appropriate safeguards — Ethics Committees operating within that national legal framework should not routinely require individual informed consent as a separate ethical precondition.. The EDPB encourages national supervisory authorities to issue guidance to Ethics Committees clarifying the relationship between ethical consent requirements and GDPR legal bases."

COMMENT 3

Reference: § 100 (Disproportionate effort) and §§ 146-164 (Appropriate safeguards)

Issue: The concept of "disproportionate effort" does not concern the financial capacity of the research institution, but only technical difficulty

The Guidelines at § 100 identify "disproportionate effort" as a ground for exemption from individual notification under Art. 14(5)(b) GDPR. The examples given focus on the **number of data subjects** and **age of the dataset** as indicators of disproportionality.

However, the Guidelines do not address the **financial dimension** of disproportionality. For a funded commercial sponsor, contacting 10,000 patients is a significant but manageable cost. For an unfunded non-profit NHS investigator, the same task may represent an **absolute financial impossibility**, irrespective of the technical feasibility.

The current framing risks creating a system in which compliance is achievable only for research with strong commercial backing — precisely the type of research that is least in need of data protection facilitation, as it has the resources to implement all required measures.

Suggested amendment to § 100:

Please consider the inclusion of the following factor to the non-exhaustive list of circumstances indicating disproportionate effort:

"The financial and organisational capacity of the controller, in particular where the controller is a non-profit public institution conducting investigator-initiated research without dedicated research funding, and where the cost of individual notification would consume resources that would otherwise be necessary for the conduct of the research itself or would require external funding that is unavailable."

COMMENT 4

Reference: §§ 146-170 (Appropriate safeguards, Art. 89(1) GDPR)

Issue: The safeguard catalogue should explicitly recognise Ethics Committee waiver approval as a sufficient primary safeguard for non-profit retrospective research on pseudonymised data

The Guidelines at § 170 provide a rich catalogue of safeguards. However, they do not explicitly address the situation — common in non-profit academic research — where:

- the data is already pseudonymised at collection,
- the research is retrospective and non-interventional,
- an Ethics Committee has reviewed the project and granted a waiver of individual consent,
- the controller is a public non-profit institution with no commercial interest in the data.

In this configuration, the combination of pseudonymisation and Ethics Committee approval constitutes a robust safeguard structure that is at least equivalent to — and in some respects more rigorous than — a consent-based approach.

The Guidelines should recognise this configuration explicitly, rather than leaving controllers uncertain as to whether additional measures are required.

Suggested addition to § 170:

"Where personal data processed for scientific research purposes are pseudonymised prior to processing, the research is retrospective and non-interventional, and a favourable opinion has been obtained from an independent Ethics Committee that has specifically reviewed and approved the absence of individual consent, this combination of safeguards may, depending on the risk profile of the specific research, constitute a proportionate and sufficient safeguard structure pursuant to Art. 89(1) GDPR, without requiring additional consent management infrastructure. This is particularly the case for non-profit public research institutions"

COMMENT 5

Reference: §§ 5-9 (Scope), §§ 63-75 (Special categories), §§ 146-170 (Safeguards)

Issue: The Guidelines do not address the specific situation of mixed datasets containing data of both living and deceased patients — a structural feature of long follow-up retrospective studies

The gap: The Guidelines are silent on the processing of personal data of deceased persons, despite this being one of the most frequent and practically significant issues in retrospective medical research. Under Recital 27 GDPR, the Regulation does not apply to personal data of deceased persons. Member States may provide national rules.

The practical consequence: A controller conducting a retrospective study on a mixed dataset of living and deceased patients operates under two simultaneous and structurally different legal regimes:

- For **living patients**: the full GDPR framework applies, including the need for a legal basis under Art. 6(1), a derogation under Art. 9(2) for health data, transparency obligations, and safeguards under Art. 89(1)
- For **deceased patients**: the GDPR does not apply; national law governs — in Italy, this means professional medical secrecy (Art. 10, FNOMCeO Code of Medical Ethics), the Garante's Provvedimento n. 298/2024, and Ethics Committee approval under Art. 110 of the Privacy Code

The problem of Ethics Committees: deceased patients cannot consent, their families may be untraceable, and any requirement introduces severe selection bias by excluding precisely those patients whose absence from the dataset — due to death — may be the scientifically most relevant data point.

Suggested addition — new paragraph within Section 2 or as a dedicated sub-section:

"Where a retrospective research dataset contains personal data of both living and deceased persons, controllers should apply the GDPR framework exclusively to the data of living persons, in accordance with Recital 27 GDPR. Personal data of deceased persons is not subject to the GDPR; its processing is governed by applicable national law, including professional secrecy obligations and any national rules adopted by Member States pursuant to Recital 27. Controllers are not required to obtain a GDPR legal basis, an Art. 9(2) derogation, or individual consent for the processing of personal data of deceased persons for scientific research purposes."

"Where personal data of deceased patients includes genetic or hereditary information that may indirectly reveal health-related data concerning living relatives, controllers should assess whether those living relatives are identifiable from the dataset and, if so, apply the GDPR framework to that derived or inferred data. This assessment should be documented as part of the risk analysis required under Art. 89(1) GDPR and §§ 151-153 of these Guidelines."

GENERAL REMARK

The undersigned respectfully submits that the current Guidelines, while representing a significant and welcome step forward in providing clarity on scientific research under

the GDPR, do not adequately address the structural disadvantage faced by non-profit public research institutions where public research may be underfunded.

The GDPR and the Guidelines both recognise that scientific research is a societal good. The practical effect of a uniform compliance framework — applied identically to a commercial profit company and to an unfunded NHS or underfunded academic investigator — is to privilege commercial research over public research. This is contrary to the spirit of Art. 179 TFEU and Recital 159 GDPR.

Unfunded research in high-impact medical journals decline over recent decades is itself a structural concern: industry-funded studies more than doubled from 17% to 40% in high-impact journals over a 20-year period, while government-funded studies remained constant and non-funded studies declined. Unfunded public academic research covers terrain that commercially funded research structurally cannot or will not occupy, such as rare diseases and low-prevalence conditions, emergency medicine and real-world clinical practice data.

Indeed please consider issuing, alongside or following the finalisation of these Guidelines, **specific guidance on non-profit public research**, addressing in particular:

1 A lighter, proportionality-based safeguard regime for non-funded investigator-initiated research on pseudonymised data
2 Guidance to national Ethics Committees on the relationship between ethical consent requirements and GDPR exemptions
3 Explicit recognition that financial impossibility of consent management constitutes "disproportionate effort" under Art. 14(5)(b) GDPR