AN A.S. PRATT PUBLICATION
JULY-AUGUST 2025
VOL. 11 NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 6** **July-August 2025**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2025–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

European Health Data Space Regulation Published in the EU Official Journal

By Alexander Roussanov and Ana Gonzalez-Lamuño*

In this article, the authors analyze the final text of the European Health Data Space regulation, focusing on the key elements relevant to the secondary use of health data for Life Sciences companies.

Regulation 2025/327 (EHDS Regulation), creating a European Health Data Space (EHDS), has been published[1] in the European Union Official Journal (EU Official Journal), marking the end of the legislative process of the EHDS Regulation.

BACKGROUND

The EHDS Regulation is based on the European Commission proposal for a Regulation creating a European Health Data Space, published in May 2022. The European Commission proposal underwent substantial amendments by the European Parliament and Council of the European Union (EU legislators) as a result of intense debates. The debates touched upon, among other things, the possibility for EU citizens to object (opt-out) to the collection and use of their health data and to consent (opt-in) in specific cases. Another sensitive topic was the ability of the EU Member States to opt-out from the EHDS and to introduce additional restrictions to the use of health data.

The EU legislators reached an agreement on the text of the EHDS Regulation on March 15, 2024. It was then formally adopted by each of the EU legislators separately on April 24, 2024, and January 21, 2025.

The EHDS Regulation establishes rules for the:

- Access to electronic health data (health data) for healthcare purposes (i.e., primary use)
- Sharing and access of specific electronic health data for purposes other than the initial purposes for which the data was initially collected or produced (i.e., secondary use)

Life Sciences companies can apply for access to health data (health data applicant) for secondary use, but primary use is restricted to patients and healthcare professionals. At the same time, Life Sciences companies are required to share certain health data they hold when acting as data holders (health data holder).

* The authors, attorneys with Arnold & Porter Kaye Scholer LLP, may be contacted at alexander.roussanov@arnoldporter.com and ana.lamuno@arnoldporter.com, respectively.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202500327.

This article analyzes the final text of the EHDS Regulation, focusing on the key elements relevant to the secondary use of health data for Life Sciences companies.

KEY ELEMENTS OF THE EHDS REGULATION AND ITS RELEVANCE FOR COMPANIES

The EHDS Regulation officially establishes HealthData@EU, a cross-border infrastructure enabling the secondary use of health data, which has been operational as a pilot since 2022. This platform will maintain a publicly available EU dataset catalogue, listing the health data that may be requested for secondary use.

Obligations for Health Data Holders

The EHDS Regulation introduces the concept of "health data holder," which can include any legal person operating in the healthcare sector, developing health products or services, or conducting health-related research, as well as public authorities, agencies, and bodies, including reimbursement services that either:

- Has the right or obligation to process personal health data, or
- Has the ability to make non-personal health data available

Life Sciences companies handling health data may qualify as health data holders. Natural persons and microenterprises (i.e., enterprises employing fewer than 10 people and with an annual turnover or balance sheet of less than €2 million) are excluded from qualifying as health data holders. However, EU Member States may extend the obligations for health data holders to natural persons and microenterprises.

Key obligations for health data holders include:

- *Obligation to Share Health Data*: When access to health data is granted by the health data access body (HDAB, a national body responsible for assessing health data access requests and applications), health data holders must share the requested health data, unless the patients concerned have opted out of sharing. The data must be shared with the HDAB of the health data holder's country of establishment within three months. The HDAB will then provide access to the health data applicant who has been granted access, who will only be able to download non-personal health data.
- *Obligation to Communicate the Dataset*: Health data holders must inform the HDAB of their country of establishment about the datasets they hold and ensure that the dataset descriptions in the national dataset catalogue are accurate and up to date, at least annually.

Possibility to Access Health Data for Secondary Use

The EHDS Regulation introduces the concept of a "health data applicant," which can include any natural or legal person established in the EU (or, under certain criteria, in a non-EU country). Health data applicants are eligible to request access to health data, but access is only granted if deemed lawful by a HDAB. The HDAB evaluates requests based on criteria such as: intended use, purpose, safeguards against data misuse, compliance with the General Data Protection Regulation, or justification for relying on a national exception to the opt-out right (if applicable).

Access Routes

Access requests must be submitted to the relevant HDAB (i.e., the one where the health data holder holding the data intended to be accessed is registered). The EHDS offers different access routes, which vary in terms of the data access format (i.e., anonymized/pseudonymized format or statistical format) and processing time.

- Health Data Request:
  - *Access format:* Access to data is granted in anonymized statistical format.
  - *Timeframe:* Six months.
  - *Outcome:* If successful, HDAB grants an approval.
- Health Data Application:
  - *Access Format:* Access to data is granted in anonymized or pseudonymized format (the latter when justified only).
  - *Timeframe:* Three to six months.
  - *Outcome:* If successful, the HDAB issues a data permit valid for up to 10 years (extendable for an additional 10 years).
- Simplified Procedure: When health data is held by a designated trusted health data holder (i.e., designated by an EU Member State when meeting certain conditions such as having a secure processing environment or expertise in handling data access applications/requests), health data applicants may follow the simplified route. The trusted health data holder conducts an initial assessment and sends a recommendation to the HDAB.
  - *Access Format:* Dependent on whether it is a request or an application (i.e., anonymized statistical format, or anonymized or pseudonymized format).
  - *Timeframe:* Four months.

– *Outcome:* If successful, the outcome depends on whether it is a request or an application (i.e., an approval or a data permit).

For data held by health data holders across multiple EU Member States, health data applicants can submit a single data application, either:

- Through the HDAB of the health data applicant's EU Member State of its main establishment, or
- Through the European Commission's HealthData@EU services

Data permits issued by one HDAB may also be recognized by other HDABs.

Use for a Permitted Purpose

The EHDS Regulation allows health data to be used for the following secondary purposes:

- Public interest in the areas of public or occupational health;
- Policymaking;
- Statistics;
- Education;
- Scientific research; and
- Health treatment optimization.

For Life Sciences companies, scientific research is the key permitted purpose. The EHDS Regulation provides that scientific research should be interpreted "in a broad manner, including technological development and demonstration, fundamental research, applied research and privately funded research."[2] At the same time, scientific research must:

- Contribute to public health or health technology assessments, or
- Ensure high levels of quality and safety of healthcare, medicines, or medical devices, with the aim of benefitting end-users (e.g., patients, health professionals, and health administrators), and
- Include the development and innovation of products or services, or
- Train, test and evaluate algorithms, including in medical devices, in vitro diagnostic medical devices, AI systems, and digital health applications.

[2] EHDS Regulation Recital 61.

The EHDS provides examples of scientific research for public interest, such as "research addressing unmet medical needs, including for rare diseases, or emerging health threats."[3]

Health Data Categories Concerned by the EHDS Regulation

The EHDS Regulation specifies the categories of health data that health data holders must share, and which may be requested for access, including:

- Genetic, epigenomic, genomic, proteomic, transcriptomic, metabolomic, lipidomic, and other 'omic data;
- Data from clinical trials, clinical studies, clinical investigations, and performance studies (note that clinical trial and clinical investigations data may be shared once the trial has ended);
- Personal health data automatically generated through medical devices and "other" health data from medical devices (note that it is not specified what "other" means);
- Health data from biobanks and associated databases;
- Healthcare-related administrative data, including on dispensations, reimbursement claims, and reimbursements;
- Data from registries for medicinal products and medical devices;
- Data from medical and mortality registries;
- Data from population-based health data registries (i.e., public health registries);
- Data from health research cohorts, questionnaires, and surveys after the first publication of the results;
- Data on professional status, and on the specialization and institution of health professionals involved in the treatment of a natural person; and
- Data from wellness applications.

These are the minimum categories of health data concerned by the EHDS Regulation, though EU Member States may add additional categories of health data at the national level.

Protections

The EHDS Regulation acknowledges that health data may be protected by intellectual property rights (IPR), trade secrets, or regulatory data protection (RDP). Health data holders must inform the HDAB about these protections and justify their necessity.

[3] EHDS Regulation Recital 54.

For clinical trial and clinical investigations data, the EHDS Regulation adopts a more cautious approach, stating that such data "should be made available to the extent possible, while taking all necessary measures to protect intellectual property rights and trade secrets."

The HDAB ultimately determines whether the health data requires protection measures before being shared, and specifies the applicable measures (i.e., legal, organizational and technical measures, or contractual arrangements between health data holders and health data applicants). If the HDAB concludes that sharing the health data poses a serious risk to IPR, trade secrets, or RDP, it may reject the data application/request.

International Health Data Transfers

The EHDS Regulation allows health data applicants established in non-EU countries to request access to health data if their country:

- Complies with the EHDS Regulation;
- Provides health data applicants established in the EU access on terms and conditions equivalent to those of the EHDS Regulation; and
- Has confirmation from the European Commission that the two criteria are met.

For international transfers of non-personal health data (as referred to in Article 88 of the EHDS Regulation) from the EU to a non-EU country, the EHDS Regulation classifies data as highly sensitive if there is "a risk of re-identification through means going beyond those reasonably likely to be used, in particular in view of the limited number of natural persons to whom those data relate, the fact that they are geographically scattered or the technological developments expected in the near future."[4] Specific conditions for such international transfers of highly sensitive data will be set out in a future delegated act under the EU Data Governance Act, which has not yet been adopted.

Other Elements

Other elements that may be relevant for Life Sciences companies include:

- *Stricter National Measures*: EU Member States may impose stricter measures and safeguards for sensitive data categories (e.g., genetic data and health data from biobanks).
- *Obligation to Publish Results of Data Use*: When health data is used for secondary purposes, the results of the use must be published within 18 months in an anonymized format.
- *Penalties*: Health data holders and users of health data for secondary use who fail to comply with the EHDS Regulation may face penalties from

[4] EHDS Regulation Article 88.1.

HDABs, such as exclusion from accessing health data for up to five years, or penalty payments.

- *Gradual Application of the EHDS Regulation*:
  - *Primary Use and General Provisions*: The EHDS Regulation will apply two years after it becomes law (i.e., March 25, 2027). This includes provisions on primary use, and other provisions such as regarding international health data transfers and non-personal health data requests.
  - *Secondary Use*: Provisions on the secondary use of the data (except for specific data such as human genetic, molecular, or clinical trials data) will apply four years after the EHDS Regulation becomes law (i.e., March 25, 2029).
  - *Previously Excluded Data*: Provisions on secondary use of previously excluded data types (e.g., genetic, molecular, or clinical trials data) will apply six years after the EHDS Regulation becomes law (i.e., March 25, 2031).

HOW COMPANIES CAN PREPARE

The implementation of the EHDS Regulation is likely to raise unresolved questions, which future European Commission implementing regulations or guidelines may clarify. Some uncertainties include: the criteria that HDABs will use to decide on the protection of sensitive and confidential information, or how the opt-out mechanism for patients will be handled.

Companies that may qualify as health data holders should prepare ahead of the application of the EHDS Regulation by adapting and setting up internal procedures and policies (e.g., with data redaction procedures and identifying the data subject to the sharing obligations under the EHDS Regulation). Additionally, companies could also train the relevant personnel on the practical aspects of the EHDS. These steps may help ensure compliance and allow companies to take full advantage of the opportunities for accessing health data under the EHDS Regulation.

NEXT STEPS

The EHDS Regulation became law on March 25, 2025, 20 days after its publication in the EU Official Journal.

To facilitate a harmonized implementation of the EHDS Regulation, guidelines on the secondary use of health data will be published and open for consultation[5] in Autumn 2025 and Spring 2026.

[5] https://tehdas.eu/public-consultations/.