POLICY TITLE: European Economic Area and United Kingdom Data Protection Laws Policy	SYSTEM POLICY AND PROCEDURE MANUAL
POLICY #: 800.59	**CATEGORY:** Compliance & Ethics
System Approval Date: 09/19/2024 **Site Implementation Date:** 11/04/2024	**Effective Date:** 07/15/2021 **Last Reviewed/Approved:** 05/24/2023
Prepared by: Office of Corporate Compliance; Office of Research Compliance; Office of Legal Affairs	**Notations:** N/A

GENERAL STATEMENT OF PURPOSE

The purpose of this document is to describe the scope and general requirements of certain international data protection regulations enacted in the European Economic Area ("EEA") and the United Kingdom ("UK") that may apply to business, clinical and/or research activities of Northwell Health.

POLICY

It is the policy of Northwell Health to protect the privacy and security of Personal Data and to comply with all applicable laws and policies relating to data privacy and information security.

The EEA General Data Protection Regulation ("GDPR") and the UK Data Protection Act 2018 ("DPA18," and together with GDPR, the "EEA/UK Data Protection Regulations") require organizations to protect and secure Personal Data of natural persons in the EEA and the UK and to implement and adhere to certain procedures with respect to the processing and sharing of Personal Data, privacy notices, breach notification, security requirements and Data Subject rights, as herein defined.

Because the EEA/UK Data Protection Regulations may apply to Northwell Health activities, including those taking place *within* the United States, (1) the Office of Legal Affairs and/or the Office of Corporate Compliance must be consulted in advance to determine whether Northwell Health's proposed business activities involving Processing Personal Data fall within the territorial scope of the EEA/UK Data Protection Regulations, and (2) the Office of Research Compliance must be contacted for proposed Processing activities involving research related to EEA/UK Data Subjects.

For more general information about the EEA/UK Data Protection Regulations, please refer to the section *General Information About the EEA/UK Data Protection Regulations*, below.

SCOPE

This policy applies to all Northwell Health employees, as well as medical staff, volunteers, students, trainees, physician office staff, contractors, trustees and other persons performing work for or at Northwell Health; faculty and students of the Donald and Barbara Zucker School of Medicine at Hofstra/Northwell or the Hofstra Northwell School of Nursing and Physician Assistant Studies conducting research on behalf of the Zucker School of Medicine on or at any Northwell Health facility.

DEFINITIONS

Adequacy Decision: A decision adopted by the European Commission on the basis of Directive 95/46/EC, which establishes that a non-EU country ensures an adequate level of protection of Personal Data by reason of its domestic law or the international commitments into which it has entered.

Anonymized Data: Personal Data that has been rendered anonymous, meaning that it is not possible to identify the Data Subject, and technical safeguards are in place such that data can never be re-identified.

Biometric Data: Personal Data resulting from specific technical Processing relating to the physical, physiological, or behavioral characteristics of an individual, which allows for, or confirms, the unique identification of that individual, such as facial images or fingerprinting data.

Consent: freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which the Data Subject, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to the Data Subject.

Controller: a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Data Concerning Health: Personal Data related to the physical or mental health of an individual, including the provision of health care services, which reveals information about the individual's health status.

Data Subject: a natural person (i.e., living human being) that is not a corporate or organizational entity.

EEA: the European Economic Area, consisting of European Union (EU) Member States and countries with ratified membership in the Union, which together includes: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

EEA/UK Representative: a natural or legal person established in the EEA/UK who, designated by the Controller or Processor in writing, represents the Controller or Processor with regard to the Controller or Processor's, as applicable, respective obligations under GDPR and/or the DPA18.

Genetic Data: Personal Data relating to the inherited or acquired genetic characteristics of an individual which give unique information about the physiology or the health of that individual and which result, in particular, from an analysis of a biological sample from the individual.

Personal Data: any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

Processing: any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available alignment or combination, restriction, erasure or destruction.

Processor: a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller.

Pseudonymized Data or Pseudonymization: data (or coded data) that has been processed such that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information and that additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

Special Categories of Personal Data or Sensitive Personal Data: data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, Genetic Data, Biometric Data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Supervisory Authority: an independent public authority which is established by a Member State pursuant to Article 51 of GDPR. For the purposes of this policy, this shall include the UK Information Commissioner's Office.

UK: the United Kingdom of Great Britain and Northern Ireland, consisting of the following countries: England, Scotland, Wales and Northern Ireland.

PROCEDURE

When Northwell Health seeks to engage in activities with a third party that involve or may involve Processing Personal Data from individuals located in the EEA and/or UK or that involve or may involve the receipt of data from or the accessing of data held by an EEA or UK site (e.g., research registry data), the Office of Legal Affairs must be contacted before contracting or otherwise engaging in those activities with that third party for a determination as to whether and to what extent the EEA/UK Data Protection Regulations apply. In addition, all business conducted with third-party Vendors must comply with Policy 300.26 Procurement of Goods and Services and Policy 300.16, Vendor Screening and Compliance.

The Office of Legal Affairs will assess the applicability of EEA/UK Data Protection Regulations by determining whether Personal Data is involved and whether the activity falls within the scope of the EEA/UK Data Protection Regulations. Personal Data is defined to include Pseudonymized Data (or coded data) but not Anonymized Data.

If the EEA/UK Data Protection Regulations apply, the Office of Legal Affairs will advise as to the appropriate form of contract between Northwell Health and the third party. This will depend, in part, on whether the other party is a Controller (independent or joint) or a Processor (in each case within the meaning of the EEA/UK Data Protection Regulations). It will also depend on the volume, type and sensitivity of the Personal Data Northwell Health will handle.

The Office of Research Compliance must be contacted for proposed research related activities involving EEA/UK Data Subjects. The Office of Corporate Compliance also must be contacted for consultations regarding any other proposed activities involving EEA/UK Data Subjects.

Data Protection Officer

In certain cases when Northwell Health acts as Controller or Processor requiring appointment of a Data Protection Officer ("DPO"), the Senior Vice President and Chief Corporate Compliance Officer will designate the DPO for Northwell Health. The designation of such individual(s) shall be recorded in the minutes of the Executive Audit and Corporate Compliance Committee.

Once appointed, the Data Protection Officer ("DPO") is responsible for the development and implementation of the policies and procedures required to comply with GDPR and/or the DPA18 where the core activities of the Controller or Processor consist of certain Processing operations such as regular and systematic monitoring of Data Subjects on a large scale or Processing special categories of data on a large scale.

The DPO shall oversee and coordinate with Northwell Health's Digital IT and Services and the Corporate Security and Support Services departments and other applicable department personnel related to privacy and security. The DPO will advise Controllers and/or Processor on their obligations, monitor for compliance, coordinate with any Supervisory Authority, and undertake any other responsibilities as required pursuant to the EEA/UK Data Protection Regulations.

Breach Notification

You must contact the Office of Corporate Compliance immediately upon becoming aware of any

incident you think is, or may be, a Personal Data Breach—even if you are unsure whether a breach has happened or is happening and/or whether it involves Personal Data. In addition, IT Security must be contacted through the Digital IT&S Service Desk for any IT security related incidents.

Corporate Compliance will determine whether a Personal Data Breach should be reported to the Supervisory Authority, affected Data Subjects or third parties, or otherwise disclose details of (including the existence or suspected existence of) any Personal Data Breach to any affected person.

In the case of a Personal Data Breach, where Northwell Health acts as the Controller, Northwell Health shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, report the Personal Data Breach to the appropriate Supervisory Authority including all required elements, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Supervisory Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The notification by the Controller shall at least:

a) Describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
b) Communicate the name and contact details of the DPO or other contact point where more information can be obtained;
c) Describe the likely consequences of the Personal Data Breach; and
d) Describe the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where Northwell Health acts as a Processor, Northwell Health shall notify the Controller without undue delay after becoming aware of a Personal Data Breach relating to its Processing for that Controller.

<u>Communication to the Data Subject by the Controller</u>

When the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons, Northwell Health shall communicate the Personal Data Breach to the Data Subject without undue delay. The communication shall describe in clear and plain language the nature of the Personal Data Breach and contain at least the information (b), (c) and (d) above.

Communication to the Data Subject shall not be required if one or more of the following conditions are met:

- Northwell Health has implemented appropriate technical and organizational protection measures, and those measures were applied to the Personal Data affected by the Personal Data Breach, in particular those that render the Personal Data unintelligible to any person who is not authorized to access it, such as encryption;
- Northwell Health has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialize; or

- It would involve disproportional effort. In such cases, there shall instead be a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner.

GENERAL INFORMATION ABOUT THE EEA/UK DATA PROTECTION REGULATIONS

The following summarizes key features of the EEA/UK Data Protection Regulations and is provided for information.

A. Territorial Scope of the EEA/UK Data Protection Regulations

As enacted, the EEA/UK Data Protection Regulations apply to the Processing of Personal Data by entities that:

1) Are established in the EEA/UK under Article 3(1) GDPR/Section 207(2) DPA18; or
2) Are established only outside the EEA/UK but offer goods or services to, or monitor the behavior of, individuals in the EEA/UK under Article 3(2) GDPR/Section 207(3).

Currently, Northwell Health does not maintain an EEA/UK establishment. Therefore, the EEA/UK Data Protection Regulations will only apply to Northwell Health, if at all, under the second prong.

B. Controllers and Processors

The EEA/UK Data Protection Regulations apply to, and regulate, entities as either *Controllers* or *Processors*. Controllers and Processors are subject to specific regulatory responsibilities.

1) Based on Northwell Health's current and proposed activities, Northwell Health may be considered a **Controller** under the Regulations in the following scenarios (this list is not exhaustive):
    - Sponsoring research and/or clinical trial studies with sites located in, or involving Data Subjects within, the EEA and/or UK (e.g., an investigator-initiated research study sponsored by Northwell Health);
    - Sponsoring registry or survey studies located in, or involving Data Subjects from, the EEA and/or UK;
    - Directing, sponsoring, or administering an international patient program that attempts to reach, market to, and provide services to Data Subjects from the EEA and/or UK including through use of telehealth services; or
    - Providing webinars and sending marketing materials to, and using cookies and similar technologies for the purposes of tracking, HCPs and other individuals in the EEA and/or UK.

2) Based on Northwell Health's current and proposed activities, Northwell Health may be considered a **Processor** under the Regulations in the following scenarios (this list is not exhaustive):

    - Acting as a contract research organization or other vendor of clinical research services for Controllers that are based in the EEA and/or UK

- Acting as a service supplier or provider to Controllers that are subject to GDPR and/or DPA18 — irrespective of where these Controllers are established.

C. Local Representative

When acting under the EEA/UK Data Protection Regulations as a Processor or a Controller of Personal Data, Northwell Health may need to designate a representative established in the EEA/UK.

D. Cross-Border Transfer of Personal Data Outside the EEA/UK

Since the U.S. lacks an Adequacy Decision by the European Commission, transfers of Personal Data to third countries and onward transfers to other third countries require adequate safeguards or appropriate derogations (or exceptions) for specific situations.

E. Heightened Protections

1) Special Categories of Personal Data. The EEA/UK Data Protection Regulations prohibit the Processing of Special Categories of Personal Data unless certain requirements and heightened protections are met. Special categories of Personal Data include racial or ethnic origin; Data concerning Health; political opinions, religious or philosophical beliefs; trade union membership; sex life or sexual orientation; Genetic Data; and Biometric Data.

2) Minors. When seeking to Process Personal Data to offer online services directly to a minor or child below the age of 16 in the EEA, such Processing shall be lawful only if, and to the extent, that Consent is given or authorized by a holder of parental responsibility over the child.

F. Data Subject Rights and Requests

Under the EEA/UK Data Protection Regulations, Data Subjects have a number of rights regarding the Processing of their Personal Data. Some of these rights only apply where a specific set of conditions have been met and no applicable exemptions are available, whereas others are absolute and can be exercised by the Data Subject without restriction. These rights are:

- **Access**: The right to obtain confirmation from Northwell Health about whether or not it processes Personal Data about the Data Subject, and, where that is the case, to receive a copy of the Personal Data;
- **Rectification**: The right to ask Northwell Health to rectify inaccurate Personal Data or fill in incomplete data relating to the Data Subject;
- **Erasure**: The right to ask Northwell Health to erase Personal Data about the Data Subject without undue delay (also referred to as the "right to be forgotten");
- **Restriction**: The right to ask Northwell Health to tag Personal Data about the Data Subject in order to restrict the Processing of the data in the future;
- **Portability**: The right to ask Northwell Health to provide Personal Data about the Data Subject in a structured, commonly used and machine-readable format

and to transmit the data to another Controller;

- **Objection (General)**: The right to object to Northwell Health's Processing of Personal Data about the Data Subject in certain cases; and
- **Objection (Automated decision-making)**: The right for a Data Subject not to be subject to a decision by Northwell Health based solely on automated processing (including profiling), where this decision has legal or other significant consequences for the Data Subject.

You must contact Corporate Compliance as soon as possible upon receiving a Data Subject rights request or inquiry to assist with evaluating and responding to the request/inquiry. Corporate Compliance will review the request and communicate to the Data Subject actions taken in response to their request without undue delay within one month of receipt of request. This period may be extended by two further months where necessary, in which case the Data Subject will be notified of the extension along with the reason for the delay within one month of the receipt of the request. If no action is taken, Northwell Health shall inform the Data Subject without delay and at least within one month of receipt of the request of the reasons for not taking action and the possibility of filing a complaint with the Supervisory Authority and seeking a judicial remedy.

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

- The General Data Protection Regulation (EU) 2016/679
- The Data Protection Act 2018
- The European Data Protection Board Guidelines 3/2018 on the territorial scope of GDPR (Article 3) – Version 2.0, 12 November 2019
- Northwell Health Policy #900.19 IT Incident Response Policy
- Northwell Health Policy #300.26 Procurement of Goods and Services
- Northwell Health Policy #300.16, Vendor Screening and Compliance

CLINICAL REFERENCES/PROFESSIONAL SOCIETY GUIDELINES

N/A

ATTACHMENTS

N/A

FORMS

N/A

APPROVALS:	
Northwell Health Policy Committee	07/23/2024
System PICG/Clinical Operations Committee	09/19/2024

Standardized Versioning History:

Approvals: * =Northwell Health Policy Committee; ** = PICG/Clinical Operations Committee; ◙ = Provisional; ❖ = Expedited

*06/24/21 **07/15/21

*04/25/23 **05/24/23