WMCM UKSW

Wydział Medyczny. Collegium Medicum
UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO
W WARSZAWIE

Legal Aspects of eIDAS 2.0 Adoption in Healthcare

Electronic Identification Schemes and the European Digital Identity Wallet

Bartłomiej Michalak
Faculty of Medicine, Collegium Medicum, Cardinal Stefan Wyszyński University in Warsaw
Polish Telemedicine and e-Health Society

Krzysztof Świtała, PhD
Faculty of Law and Administration, Cardinal Stefan Wyszyński University in Warsaw

International Online Session "One Digital Health & Artificial Intelligence" · July 11th, 2026

Polish Telemedicine Society
Polskie Towarzystwo Telemedycyny i e-Zdrowia

CONTEXT & MOTIVATION

Why Electronic Identity in Healthcare?

eHealth is now mission-critical: COVID-19 shifted outpatient care to remote delivery; in Poland this often meant simple phone teleconsultations rather than mature nationwide telemedicine.

Demography drives digitalisation: Ageing European populations and shortages of medical professionals make eHealth indispensable for maintaining quality of care.

Identity is the entry point: EHR, e-prescriptions and teleconsultations cannot function without reliably knowing who is accessing health data - patient, professional or system.

Law must keep pace: Requirements are dispersed across EU internal-market and health legislation - a source of potential inconsistency and legal risk.

CONCEPTUAL FRAMEWORK

eHealth, Telemedicine and EHR

eHealth (WHO)

Use of ICT in health care: treating patients, research, education, disease detection and population health monitoring. Includes management tools and processes - not only technology.

Telemedicine (EU)

Healthcare provided via ICT where professional and patient are not in the same location: teleconsultation, telesurgery, teleradiology, telemonitoring.

EHR

Secured set of electronic patient data with defined structure, processed for healthcare purposes. In Poland mandatory in electronic form since 2019; signed with qualified / trusted / personal signature.

Conclusion: eHealth encompasses both telemedicine and EHR - and none of it works without electronic identity management.

DEFINITIONS

Electronic Identity: Core Concepts

Identity (ISO/IEC 24760-1)
A set of attributes related to an entity relevant for the operation of a domain - persons, but also ICT systems and web services.

Electronic identification (eIDAS, Art. 3(1))
The process of using data in electronic form that uniquely identifies a natural or legal person (or a natural person representing a legal person).

Identity management (ISO/IEC 27001 - Requirements and 27002 - information security controls)
Enables unique identification of individuals and systems accessing information assets and the appropriate assignment of access rights.

Why it matters in eHealth

Secure, efficient, automated access to eHealth systems; remote public services in telemedicine; fewer visits motivated by formal - not medical - reasons.

EU LEGAL FRAMEWORK

From eIDAS to eIDAS 2.0

2014

eIDAS Reg. (EU) No 910/2014

Electronic identification & trust services: e-signatures, e-seals, certificates ensuring authenticity, integrity, non-repudiation and accountability. Notified eID schemes (Art. 9(1)).

2024

eIDAS 2.0 Reg. (EU) 2024/1183

European Digital Identity Framework: extended harmonisation, improved security of trust services, normative definition of the European Digital Identity Wallet.

2026

National implementation

In Poland: draft bill amending the Act on Trust Services and Electronic Identification (RCL No. UC122, 18 Feb 2026) to adopt the EUDI Wallet concept.

Certificates identify patients, health professionals and healthcare providers - and secure websites and web services (TLS, X.509).

EUROPEAN DIGITAL IDENTITY WALLET

A Universal Tool for Managing Personal eID

“A product and service that enables a user to store identity data, credentials and attributes, provide them on demand to relevant parties, and use them for online and offline authentication.”

Regulation (EU) 2024/1183, normative definition

Patients, professionals, researchers

EHDS couples new controller obligations with electronic identification mechanisms - including the wallet (recital 21, Reg. 2025/327).

Online & offline use

Attributes and credentials presented on demand - supporting cross-border healthcare scenarios.

Risk of dispersion

eID rules spread across internal-market and health law; eHealth Network, DPAs and ENISA must flag gaps and conflicts.

Main date of deployment in EU Member States: 6 December 2026

Potential
For European Digital Identity
Co-funded by the European Union

Potential for European Digital Identity Project

ePrescription case study

A secure digital way to fill or refill prescriptions anywhere in Europe.

The European cross-border network solution—MyHealth@EU—allows pharmacists in one country to access a patient's prescription data from another, improving convenience and continuity of care.

The introduction of ePrescriptions through the EUDI Wallet offers multiple advantages for patients, healthcare providers, and pharmacies:

- ***Seamless cross-border access**: patients can securely access and use their prescriptions, even when traveling abroad, ensuring they receive the medication they need wherever they are.*
- ***Increased efficiency**: eliminating paper forms reduces administrative burdens and waiting times for patients and pharmacists.*
- ***Enhanced security & privacy**: Data is protected under EU standards, and selective disclosure mechanisms ensure only necessary information is shared.*
- ***Better patient experience**: with digital infrastructure in place, patients benefit from a more convenient healthcare experience, including the possibility to prove eligibility for medication without revealing unnecessary personal details.*

SECTOR-SPECIFIC REQUIREMENTS

European Health Data Space - Reg. (EU) 2025/327

Article 16 Secure processing environment

Data users may access only the electronic health data they are authorised to access, and only through individual, unique user identities and confidential access modes.

Article 12 Health professionals

For priority categories of personal electronic health data (patient summaries, e-prescriptions & dispensations, medical imaging and reports), professionals must use eIDAS-compliant electronic identification means.

Accountability for access to medical databases must rest on effective, legally recognised user authentication that safeguards fundamental rights - privacy and the informational autonomy of the individual. The eHealth Network (Art. 14, Directive 2011/24/EU) promotes universal identification methods and eIDAS use in day-to-day healthcare.

HUMAN RIGHTS IN HEALTHCARE PERSPECTIVE

Patient Rights Enabled by Electronic Identity

Right to health services

Includes modern electronic processing of medical data - teleconsultation, diagnostic imaging - in line with current medical knowledge.

Consent, anywhere & anytime

Digital identity lets patients express informed consent electronically for telemedicine and traditional services - no paper form to collect and deliver.

Information & access to records

The right to medical records is the de facto basis of the right to health information - supporting genuinely voluntary decisions.

Accessibility

eID increases eHealth accessibility for people with reduced mobility, hearing or visual impairments (Directive 2016/2102, WCAG); adoption by providers is often insufficient.

INFORMATION SECURITY PERSPECTIVE

Confidentiality, Medical Secrecy and Accountability

Identify - Authenticate - Authorise: eHealth/EHR systems record who did what and when; if these processes fail, unauthorised persons must not reach protected resources.

ISO/IEC 27001 access control: Access restricted to genuinely justified cases of use, respecting necessity and proportionality - the standard for the health information system.

Medical confidentiality & autonomy: Authentication protects the patient's autonomy by effectively identifying those authorised to access health data - preserving informational self-determination.

Trust in the doctor-patient relationship: Data exchange guaranteeing confidentiality, integrity, authenticity, non-repudiation and accountability sustains service quality and trust.

CASE STUDY 1

Estonia: A Unified e-ID Ecosystem

Identity Documents Act (1999) - one act, one system:

- ID card - physical document with electronic layer
- Residence Permit card
- Digi-ID - purely digital identity (closest to the eID concept)
- e-Residency Digi-ID
- Mobiil-ID - identity verified via mobile device SIM data
- Diplomatic identity card

Used far beyond healthcare: insurance eligibility, records access, public registers, banking, transport, social benefits and voting. Health Services Organisation Act (2002) ties e-ID to the Health Information System; Terviseportaal enables enrolment, records access, teleconsultation and full lab/imaging processing over X-Road.

#1 eHealth maturity 2024 Estonia scored 100% and ranked first in the EU

84% of prescriptions were already electronic as early as 2011

X-Road unified, secure data exchange between public and private sector

CASE STUDY 2

Poland: Capable Tools, Dispersed Regulation

Profil Zaufany (Trusted Profile)

Data identifying and describing a natural person, issued under the Computerisation Act (2005). Notified under eIDAS Art. 9(1).

Profil Osobisty (Personal Profile)

Certificate-confirmed data in the electronic layer of the ID card - Act on Identity Cards (2010). Also eIDAS-notified.

mObywatel (mCitizen)

Mobile documents confirming identity and citizenship - Act of 26 May 2023. Mainly for in-person contacts with medical entities; a designated authentication tool for public ICT systems, but not an eIDAS-notified scheme.

In healthcare: authentication to the Internet Patient Account (pacjent.gov.pl) and eGabinet (gabinet.gov.pl) for professionals.
De lege ferenda: integrate these services with e-Delivery and mobile mObywatel so they are consistent in legal construction, technical requirements and interoperability.

COMPARISON

Estonia vs Poland: Comparative Assessment

Dimension	Estonia	Poland
Legal basis	Single act - Identity Documents Act (1999)	Dispersed: ID Card Act, Computerisation Act, mObywatel Act, e-Delivery Act
Architecture	Physical documents with e-layer + purely digital IDs (Digi-ID) + mobile (Mobiil-ID)	ID card with personal profile + trusted profile + m-Citizen profile
eIDAS Art. 9(1) notification	Entire system: ID card, RP card, Digi-ID, e-Residency, Mobiil-ID, diplomatic card	Only Trusted Profile and Personal Profile; mObywatel not included
Health integration	e-ID embedded in the Health Information System (Terviseportaal, X-Road)	IKP / eGabinet authentication; integration gaps remain
Maturity	Coherent and mature - normative and technical layers integrated	Capable but fragmented; interoperability doubts

CONCLUSIONS

Identity Is the Legal Backbone of eHealth

Authentication first

Verifying who the user is enables authorisation proportional to privileges - realising data protection and medical secrecy requirements.

eIDAS 2.0 & EHDS converge

The EUDI Wallet plus EHDS Articles 12 and 16 set a common direction: eIDAS-compliant eID as the default key to health data.

Coherence beats capability

Estonia shows that uniformity of legal and technical solutions matters more than the number of tools; Poland should consolidate.

Beyond hard law

Consistent regulation must be supported by technical standards and soft law - internal policies and codes of conduct.

Thank you

Krzysztof Świtała

k.switala@uksw.edu.pl

Bartłomiej Michalak

b.michalak@uksw.edu.pl

Cardinal Stefan Wyszyński University in Warsaw