SAFEPOLYMED

Safety in Polypharmacy Training Course

Session 7

Data Safety, Privacy, and GDPR

Written version of the video scripts

In this session

Video #1 — GDPR Fundamentals: Understanding Your Data Rights
Video #2 — GDPR in Health Research and Polypharmacy: From Consent to Everyday Care
Video #3 — The European Health Data Space: What's Coming Next

Original presenters: Patricia Cervera de la Cruz, Dominique Hamerlijnck, Joan Jordan, Olga Millán
Original session date: 04 November 2025

Contributors

LeukaNET
Leukemia Advocates Network

Patvocates
PATIENT ENGAGEMENT IS IN OUR DNA

AI Disclaimer

The educational content was created by humans and subsequently edited and summarised with AI assistance.

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Contents

VIDEO #1 — GDPR Fundamentals: Understanding Your Data Rights 3
1. Introduction 3
2. Main content 3
3. Key takeaways 7
VIDEO #2 — GDPR in Health Research and Polypharmacy: From Consent to Everyday Care 8
1. Introduction 8
2. Main content 8
3. Key takeaways 11
Video 2 – Part 2 12
1. Introduction 12
2. Main content 12
3. Key takeaways 13
VIDEO #3 — The European Health Data Space: What's Coming Next 15
1. Introduction 15
2. Main content 15
3. Key takeaways 19

VIDEO #1 — GDPR Fundamentals: Understanding Your Data Rights

Estimated Duration: 12–15 minutes
Target Audience: Broad: patients, caregivers, and clinicians

1. Introduction

Every time you visit a doctor, fill in a prescription, or use a health app, information about you is being collected, stored, and shared. Who is responsible for protecting it? Who is allowed to see it? And what rights do you actually have over it?

In this video, we are laying the foundation for the rest of this session: What personal data really means, and the regulation designed to protect it, the GDPR.

2. Main content

What Counts as "Personal Data"?

Let's start with the basics. Personal data means any information relating to an identified or identifiable natural person, also called a "data subject." Someone is identifiable, directly or indirectly, through things like their name, an identification number, location data, an online identifier, or even factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.

And what is "Processing"? Is the term for any operation performed on that data, automated or not. This is a much broader concept than people often assume: It includes collection, recording, storage, adaptation, retrieval, consultation, combination, restriction, disclosure, and even erasure or destruction.

Who is Responsible? Controller vs. Processor

Now two more essential terms: Controller and Processor.

The controller is the natural or legal person, public authority, or body that determines the purposes and means of processing personal data; in other words, they decide why and how the data is used. While the processor is whoever processes that data on the controller's behalf.

Let's picture a health clinic recording your personal data, your name, your visit dates, your reason for the visit. If that clinic uses a separate software provider to store and manage those records, the clinic is the controller, and the software provider is the processor, working under the clinic's instructions.

The Right to Data Protection and What the GDPR Actually Is

With all these data use and data sharing then comes data protection and your right to it.

Data protection is not just good practice. It is a fundamental right. Article 8 of the EU Charter of Fundamental Rights states that everyone has the right to the protection of their personal data; that data must be processed fairly, for specified purposes, based on consent or another legitimate legal basis. That everyone has the right to access and correct their own data; and that compliance must be overseen by an independent authority.

Now, the General Data Protection Regulation or GDPR. This is the comprehensive law that puts this right into practice. It governs how personal data of individuals within the EU is collected, processed, and stored, spanning 99 articles and 173 recitals. Its purpose is to give individuals more control over their information while making sure organisations handle that data responsibly, with meaningful penalties when they don't.

Here's what makes the GDPR so far-reaching: It applies to any company doing business in the EU, and to all personal data belonging to EU citizens or residents, regardless of where the controller or processor is based. That means people outside the EU can fall under the GDPR's protection too, and organisations worldwide need to pay attention if they handle EU residents' data.

Free Movement of Data Within the EEA

One core GDPR principle is that the free movement of personal data within the Union cannot be restricted for reasons related to data protection. But this free flow is limited to the European Economic Area or EEA, which includes all EU member states plus Iceland, Liechtenstein, and Norway. Countries outside the EU or EEA do not automatically benefit from this free flow.

Here's what that looks like in practice: If a controller in the Czech Republic stores data with a cloud provider in Norway, there is no issue, both are within the EEA. But if a controller in Spain wants to use a provider based in Switzerland, which is outside the EEA, they will need an additional legal basis, such as an adequacy decision, to justify that data transfer.

The Seven Principles of GDPR

Let's go a bit deeper.

The GDPR is built on seven core principles: Lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality, meaning security; and accountability.

Two of these, data minimisation and purpose limitation, deserve a closer look, because violations here can have real consequences. Personal data must be collected only for a specified purpose, limited to what is necessary, and it cannot later be reused for a different, incompatible purpose. Consider this real scenario: A man attends a peaceful environmental protest and is recorded by a security camera using facial recognition. That footage ends up in a law enforcement database, flagging him as a potential criminal, even though he did nothing wrong. Years later, his job applications get rejected and he is refused entry to concerts, with no idea why. When he investigates, he discovers far more data was collected and retained than was ever necessary, a breach of data minimisation; and that it was used for a purpose entirely different from the original investigation, a breach of purpose limitation. Once he raises this with his national data protection authority, his information is corrected, and the unjust consequences stop.

Legal vs. Ethical Approaches to Data Protection

It is worth distinguishing two ways of thinking about data protection. The legal and the ethical approach.

The legal approach focuses on compliance with established laws, avoiding penalties, it is rule-based, objective, and enforceable. The ethical approach goes further: It emphasises fairness, transparency, and treating informed consent as an ongoing process rather than a one-time checkbox. It is about balancing innovation with privacy and taking genuine responsibility to minimise harm, often exceeding what the law strictly requires.

Who Enforces the GDPR?

But who enforces the GDPR?

Enforcement falls to National Data Protection Authorities, or DPAs. Each EEA country has its own independent authority overseeing GDPR compliance, investigating complaints, and raising public awareness of data rights. And when data processing spans multiple EEA countries, DPAs cooperate to reach consensus.

Above them sits the European Data Protection Board, or EDPB, an independent body made up of the heads of each national DPA, plus the European Data Protection Supervisor. The EDPB ensures the GDPR is applied consistently across the EU and can issue binding decisions on cross-border cases where consensus is not reached. The European Data Protection Supervisor, or EDPS, is the EU's own independent data protection authority, monitoring how EU institutions themselves handle personal data, and providing formal guidance; for example, on how new health technology regulations should apply GDPR principles to things like joint clinical assessments or rare disease patient registries.

GDPR and New Digital Health Technologies

Technology is changing quickly, but the basic principles of data protection remain the same. The GDPR was designed to protect people's personal data, no matter what technology is being used. Whether information is stored in an electronic health record, processed by artificial intelligence, or collected through a new digital health tool, organisations must still follow the same data protection rules.

One area developing rapidly is artificial intelligence, or AI. In healthcare, AI can help analyse health data, identify patterns, and support healthcare professionals in their work. But if AI systems use personal data, organisations must make sure that data is used lawfully, that only the necessary information is collected, and that people's rights are respected

Another emerging area is neurodata, which is data generated from measuring brain activity. These technologies may be used in healthcare, rehabilitation, wellbeing, and other areas. Because this type of data can reveal very sensitive information about a person, European data protection authorities have highlighted the need for strong safeguards and careful handling.

The technologies may be new, but the principles are not. Transparency, privacy, security, and respect for individual rights remain at the heart of data protection in Europe. Whether the data

is processed by a healthcare provider, an app, or an AI system, the same fundamental GDPR principles continue to apply.

3. Key takeaways

Now you have some fundamental understanding on data safety. What personal data is, who is responsible for it, and how the GDPR protects it. The GDPR seven principles and who enforces it. This sets the stage for everything else in this session.

In our next video we are going to zoom in on something that touches all of us directly: How these rules apply to health data and health research specifically.

See you in the next one!

VIDEO #2 — GDPR in Health Research and Polypharmacy: From Consent to Everyday Care

Estimated Duration: 14–17 minutes
Target Audience: Broad: patients, caregivers, and clinicians
Video 2 - Part 1

1. Introduction

Your health data can reveal far more than a diagnosis, it can reveal your genetic makeup, your family's medical history, even predictions about your future health. That is exactly why the GDPR treats it differently from ordinary personal data.

In this video, we are exploring how data protection applies specifically to health research, what makes informed consent genuinely informed, and how the rules adapt to protect vulnerable patients.

2. Main content

Why Health Data Gets Special Protection

The GDPR recognises health data as a "special category" of data, with its own definition and dedicated safeguards. Why? Because processes that foster innovation and better healthcare, like clinical trials, mobile health tools, and more, need robust data protection to maintain people's trust and confidence. Without that trust, patients and participants simply won't engage, and the research and care that depends on their data suffers.

Genetic Data: Sensitive in a Different Way

Let's have a look at genetic and genomic data, information about a person's DNA, their unique genetic blueprint. This deserves particular attention. It can reveal health information, traits, ancestry, and even potential future medical conditions, which makes it carry a genuinely high privacy risk. It is sensitive for three specific reasons: It is deeply personal, it has real potential for misuse, and unlike most other personal data it has family implications, since your genetic information also says something about your relatives. Therefore, organisations handling this

data need to pay special attention to how securely it is stored, how it is handled, and how transparently they report on their policies.

How Does GDPR Protect Your Genomic Data?

Genetic and genomic data get GDPR's strongest layer of protection, built around four guarantees.

First, a lawful basis. This means organisations cannot use your genetic data without a valid legal reason. Because genetic data is a special category of personal data, strict conditions must be met before it can be processed.

Second, your right to know. You have the right to be informed, and organisations must explain what data they collect, why they collect it, and how it will be used.

Third, your right to withdraw. If data processing is based on your consent, you have the right to withdraw that consent at any time. Once you do, the organisation must stop using your data for that purpose, unless another legal basis or legal obligation applies

And fourth, genetic data is treated as a special category. Therefore, organisations must take appropriate measures to keep your genetic data secure and protect your privacy. Because genetic data can reveal highly personal information, GDPR requires extra safeguards when it is processed.

Together, these four guarantees are what let people trust that their genomic data will be handled ethically and securely.

The key message is simple: genetic data is among the most sensitive types of personal data, and GDPR provides additional protections to help ensure it is handled responsibly, transparently, and securely.

Legal Bases for Processing Health Data: Consent Isn't the Only Route

Here's a common misconception worth correcting: Many people assume consent is the *only* legal basis for processing health data. Well, it is not. It is one of several!

Other valid legal bases include: processing necessary for employment and social law obligations, processing to protect someone's vital interests when they can't give consent themselves, processing by non-profits for their own members, processing justified by substantial public interest, processing of data the person has already made public themselves,

processing needed to establish or defend legal claims, processing needed for direct healthcare and medical purposes under professional safeguards, processing essential for public health, like disease control; and processing for research or archiving in the public interest.

All this matters, because it means health research and care can keep moving forward even when getting explicit consent is not possible, as long as one of these other legal bases genuinely applies.

Research Ethics Consent vs. GDPR Consent

It's important to separate two related but distinct ideas: Consent to participate in research, and consent under the GDPR.

Informed consent is a powerful ethical and legal requirement for most interventional biomedical research involving human participants, rooted in the World Medical Association's Declaration of Helsinki, which sets out the ethical principles for biomedical research, including the need for free and informed consent. But GDPR consent is a separate, distinct concept. While research ethics generally treats consent as the primary basis for interventional studies, data protection law is more flexible. As we just covered, it offers multiple legal bases beyond consent alone.

What Makes Consent Truly "Informed"?

For consent to be valid under the GDPR, it must be freely given, specific, informed, and unambiguous, confirmed through a clear, affirmative action.

Freely given means the participant has a real choice, no disproportionate compensation or power imbalance pressuring them.

Specific means the information sheet clearly spells out every type of data processing involved, so participants know exactly what their data will be used for, and whether it might be reused or shared.

Informed means the information provided is genuinely valid and it doesn't have to be on paper; oral explanations, audio, or video all count, as long as the person is sufficiently informed.

And unambiguous means the consent itself is clear, explicit, and given through a deliberate action, not implied or assumed.

Here's a detail that surprises many people: Patients are sometimes required to sign two separate consent forms, one for participating in the research study itself, and a separate one specifically for allowing their personal data to be processed. Two different things.

Protecting Vulnerable Groups in Research

In this course we spoke about vulnerable groups, like children, elderly patients, or those with cognitive impairment. Well, vulnerable groups often have a diminished capacity to give informed consent, which complicates the process. So, there are three ethical principles that guide how we handle this: Autonomy, ensuring informed consent or acceptance while respecting each person's right to make informed choices and talk with their support network. Beneficence, prioritizing participants' well-being by minimising risk and maximising benefit. And justice, ensuring fair and equal treatment across all patient groups, without exploitation.

Legally, there are additional safeguards required. Children under the legal age of consent need parental or guardian consent, though their own agreement should still be sought where appropriate. For people with impaired or temporary decision-making capacity, legal representatives or family members should be involved.

In practice, this means tailoring the approach to each group: For children, using age-appropriate language and visual aids, encouraging acceptance, and ensuring parents or guardians are present. For elderly patients, accommodating sensory impairments, simplifying documents, and checking in regularly to confirm continued willingness to participate. For patients with cognitive impairment, involving family or legal guardians, using decision-making aids, and adapting the consent process to fluctuating cognitive abilities. Organisations like the International Observatory on Vulnerable People in Data Protection now focus specifically on researching and disseminating best practices in this space.

3. Key takeaways

We have now covered and learned that health data carries real power to improve care, but only when it is handled with genuine respect for consent, context, and the people it belongs to.

Let's now bring this down to earth even further and look specifically at how GDPR applies to the everyday reality of managing polypharmacy.

Video 2 – Part 2

1. Introduction

If you're managing multiple medications, chances are your health data doesn't live in just one place. It's with your GP, your pharmacist, maybe a specialist, and perhaps a medication-tracking app too. Who is making sure all that data stays protected as it moves between them?

Let's connect GDPR directly to the everyday reality of polypharmacy, and what you, as a patient or caregiver, can do about it. And we start with the basics.

2. Main content

GDPR Concepts That Matter Most in Polypharmacy

A handful of GDPR concepts become especially relevant once multiple medications and multiple providers are involved. Personal data here includes things like medical history, prescriptions, and health records, anything that can identify you. There must always be a valid legal basis for processing that data. Patients have the right to access their own data, which is particularly valuable in polypharmacy for understanding your treatments and ensuring proper medication management. Data minimisation means only the data truly necessary for managing your health and medication should be collected. And data security becomes crucial precisely because polypharmacy often means that multiple healthcare providers are involved in your care at once.

What Patients Should Be Told

Now, as a patient, you should be informed about what your data will be used for, exactly what data is being collected, whether there is ever been a data breach affecting you, how long your data will be stored, and your right to be forgotten if you change your mind, along with your other data subject rights.

Things get genuinely complicated, though, when patients are sharing data across several different initiatives and need to keep track of who has what; or when vulnerable populations are involved.

This case is not just theoretical: Patients who move between countries, or receive care in different health systems, often describe real frustration at how disconnected their health information becomes. Suddenly, a new provider has no history on them at all, which is especially critical for vulnerable groups who most need continuity of care.

GDPR in Action: Three Everyday Examples

Let's make this tangible with three real-world scenarios.

First: sharing data between providers. A patient taking multiple medications may see several healthcare providers, doctors, pharmacists, specialists. GDPR requires that data shared between them is secure, and that patients are informed about exactly who has access to their information.

Second: digital health apps and medication management. Many patients use apps to track their medication schedules. GDPR ensures these apps only collect what is genuinely necessary for the app to function, nothing more.

Third: informed consent in medication adjustments. Before adjusting or adding medications, healthcare providers must explain to patients why sharing their data is necessary and obtain consent, or justify the processing through another appropriate legal basis, especially when multiple providers are involved in the decision.

Practical Tips for Patients and Caregivers

Here's what you can actually do: keep your own records, maintain an updated list of your medications, dosages, and prescribing doctors, and know who has access to your data. Ask questions, don't hesitate to ask your healthcare providers how your data is protected and shared. Use secure channels, make sure any digital tools you use for managing medications are genuinely GDPR-compliant. And if something feels wrong, report it. If you believe your data rights are being violated, report your concern to your healthcare provider or the relevant data protection authority.

3. Key takeaways

Here some takeaways from what we have gone through in this video. We spoke about some fundamentals on GDPR in health research, informed consents in research and GDPR consent,

best practices for involving vulnerable patients in research, and some tips for your everyday polypharmacy care.

Just remember, managing polypharmacy already takes real effort, your data protection shouldn't be something you have to fight for on top of it. Know your rights, ask questions, and don't be afraid to speak up if something doesn't feel right.

In our next and final video, we will look ahead to the European Health Data Space, the next major step in how your health data will be shared and protected across the EU. See you in the next one.

VIDEO #3 — The European Health Data Space: What's Coming Next

Estimated Duration: 11–14 minutes
Target Audience: Broad: patients, caregivers, and clinicians

1. Introduction

In some countries, health records still travel by fax machine. In others, a simple QR code on your prescription lets any pharmacy in the country access it instantly. The European Health Data Space is designed to close that gap between fragmented paper trails and digital access.

In this final video of Session 7, we will look at what the EHDS actually gives you, and what it means for the future of managing polypharmacy across borders.

2. Main content

What Is the EHDS?

So, what is the European Health Data Space, or EHDS. It is a major European Union regulation that creates a single, secure digital system to share and reuse electronic health data across EU countries. The EHDS works alongside the GDPR to give people more direct control over their health data, both for their own everyday care, and to support research and innovation across the EU. Think of it as the next chapter in European health data policy: Building the digital infrastructure and legal framework to make health data genuinely portable, secure, and useful, without compromising the protections the GDPR already guarantees.

Your New Rights Under the EHDS

Together, the GDPR and EHDS give you a clear set of rights over your own health data. You can access your health data electronically, immediately, free of charge, in an easily readable and commonly used format, accessible through patient portals, computers, or smartphones, and designed to comply with the European Accessibility Act for people with disabilities. You can share your data electronically with other health professionals, for instance, when moving to a new hospital, without obstruction from previous providers. You can add your own data to your

electronic health record, for yourself or for someone who trusts you, like your child. You can request corrections to inaccurate data. You can restrict access to some or all your electronic health data. However, in vital, life-threatening situations, that data may still be made available under additional restrictions. And you can easily find out exactly which professionals have accessed your data. Each EU member state must designate a digital health authority responsible for enforcing these rights.

Cross-Border Care in Action: e-Prescriptions and MyHealth@EU

Here's what this looks like in practice: A patient travelling abroad can have their electronic prescription recognised and dispensed at a pharmacy in another EU country, without needing to carry paper records or explain their full medical history from scratch. This is made possible through MyHealth@EU, the cross-border digital infrastructure that member states are required to join, connecting national systems so patients can access and share priority health data, like patient summaries, e-prescriptions, e-dispensations, medical images, lab results, and discharge reports, wherever they are in the EU.

Primary Use of Health Data: Making the System Work

The EHDS makes a clear difference between primary use and secondary use of health data.

Let's start with primary use. This means using your health data for the purpose for which it was originally collected, such as providing healthcare, receiving a prescription, accessing treatment, or managing your care. The EHDS strengthens your ability to access your own electronic health data and, when needed, to share it with healthcare professionals involved in your care, including across EU borders.

Your health data remains stored by the organisations responsible for it, the data holder such as hospitals, clinics, pharmacies, or other healthcare providers. The EHDS supports secure access and exchange of data between trusted systems when needed for healthcare.

For all of this to function smoothly, healthcare professionals need secure access to the electronic health records of the patients they are treating and must be able to update those records when providing care. To support this, the EHDS introduces mandatory requirements for interoperability, security, and privacy, along with mandatory self-certification for electronic health record systems, helping health information systems across Europe work together more effectively.

To oversee these new rules, each Member State must designate national authorities responsible for making sure these are properly implemented and enforce the EHDS framework. These authorities will help ensure that individuals can exercise their rights and that health data is protected and used in accordance with the Regulation.

Secondary Use of Health Data: Research, Innovation, and Permits

Now, let's look at secondary use. This is the reuse of health data for purposes different from the original reason for which it was originally collected, such as research, innovation, public health, policy-making, or regulatory activities.

For example, a hospital may collect health data to provide care to patients. Later, that same data could help researchers better understand a disease, evaluate treatments, improve healthcare systems, or support the development of new medicines.

The EHDS creates a common framework that makes this possible across Europe. Instead of searching country by country, researchers will be able to find out what health datasets are available and where they are held through a shared European infrastructure. The data itself is not stored in one central European database, but it can be discovered and accessed through the EHDS framework.

Of course, researchers cannot simply access the data whenever they want. They must first submit an application to a Health Data Access Body. This authority reviews the request, decides whether the intended use is allowed, and defines the conditions under which the data can be used.

And to protect privacy, the data can only be accessed in highly secure processing environments, and only in anonymised or, where genuinely necessary, pseudonymised form.

Importantly, individuals will have the right to opt out of the secondary use of their personal electronic health data. This means they can choose not to have their data used for research, innovation, or other secondary purposes, according to the mechanisms implemented by their Member State.

But there is one exception to all this, in which additional national rules may apply: Genetic data. Because genetic information is particularly sensitive, some countries may introduce extra safeguards or restrictions. This means that the availability of genetic data for cross-border research may vary across Europe

So, beyond everyday care and the primary use of health data, the EHDS also creates a secure common framework for the secondary use of health data, helping to advance research, innovation, public health, and medical knowledge across Europe.

Since we just mentioned it, it is worth being precise about the difference between two concepts, anonymisation and pseudonymisation.

Anonymisation refers to data that no longer relates to an identifiable person at all, it is a permanent, irreversible change. And pseudonymisation, on the other hand, alters data so it cannot be directly linked to someone *without* additional information, which is kept separate and protected. Critically, pseudonymous data is still considered personal data under the GDPR, it is not the same as being anonymous. And attempting to re-identify anonymised or pseudonymised individuals is strictly forbidden.

Protections Against Misuse

The EHDS also draws firm lines around what health data can never be used for, even under a valid permit. For example, it is forbidden to use this data to make decisions detrimental to individuals, to increase insurance premiums, to market health products directly to professionals or patients, or to design harmful products or services. Health data access bodies must maintain transparency, publishing information about data access applications, and researchers must make their findings public and inform access bodies of any significant health-relevant discoveries. Notably, researchers and innovators from outside the EU can access data for secondary use under the very same conditions as those within the EU, no special exceptions either way.

Your Choice: Opting Out

Finally, and very important, you always retain a choice!

Member states may offer an opt-out from cross-border data sharing for everyday care, though this does not affect how your data is digitally stored and processed within your own country's healthcare system. And if you don't want your data used for secondary purposes like research, you have the right to opt out in a simple, reversible way, though under strict safeguards, some data may still be used for genuinely important public interest purposes, with full transparency about when and why.

3. Key takeaways

This brings us to the end of Session 7 in which we have covered what personal data is, how GDPR protects it, how it applies to health research and polypharmacy, and what the EHDS means for the future.

And now you have made it through the whole SafePolyMed training series. Well done!

Over these seven sessions, we have covered the fundamentals of polypharmacy, how drugs interact in the body, the genetics behind those interactions, the factors that make patients vulnerable, how to report side effects and understand what matters most to patients, and now, how your health data is protected today, and into the future with the European Health Data Space.

The common thread throughout the training has been simple: safe, effective polypharmacy depends on informed, engaged patients working in partnership with their healthcare providers.

Thank you for joining us and helping build safer polypharmacy for everyone!

Funded by the European Union

Safety in Polypharmacy Training Course

Contributors