RECOMMENDATIONS FOR A **SECURE ACCESS** AND **EXCHANGE** OF **HEALTH DATA** IN RESEARCH PROJECTS

TECHNOLOGY

Ensure traceability of the access

Implement two-factor authentication

Use blockchain to audit and trace data exchange through peer-to-peer networks

Consider Multi-Party Computation and Federated Machine Learning when it is not possible to retrieve data from another organization

Encrypt data storage

DATA COLLECTION AND ANONYMIZATION

Conduct a double-anonymization process

Conduct a re-identification risk assessment

Follow the recommendations of your national authority

Define standard protocols and guidelines to collect and store for sharing FAIR data in Europe and make dataset interoperable

Standard ontologies must be a priority

LEGAL ASPECTS

Prove that all partners are capable of complying with GDPR

Determine the applicable national law, conditions and requirements

Define the conditions of application of national law and GDPR to the project

Train the team in the privacy value

Identify the roles played by each partner

Be accountable. Design a code of conduct: a compliance model

COMMON ASPECTS

Apply privacy and security by design and by default

Assume that full anonymization is challenging and adopt safeguards

Assess each data-sharing case-by-case by providing security and legal certainty

Prove reasonable effort on data protection compliance

Involve medical personnel in technical projects

Create legal - technical - ethical committees to issue data-sharing authorisations

BIG Medilytics

BODYPASS

DEEPHEALTH

BIG DATA VALUE PUBLIC-PRIVATE PARTNERSHIP

These projects have received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780495 (BigMedilytics), No 779780 (BodyPass), and No 825111 (DeepHealth).