ITEA 4

Project Results

Secur-e-Health

Privacy-preserving collaboration across healthcare

To enable better medical research and treatment, the ITEA project Secur-e-Health developed an array of technologies for trusted, interoperable collaboration between healthcare institutions while preserving sensitive patient data.

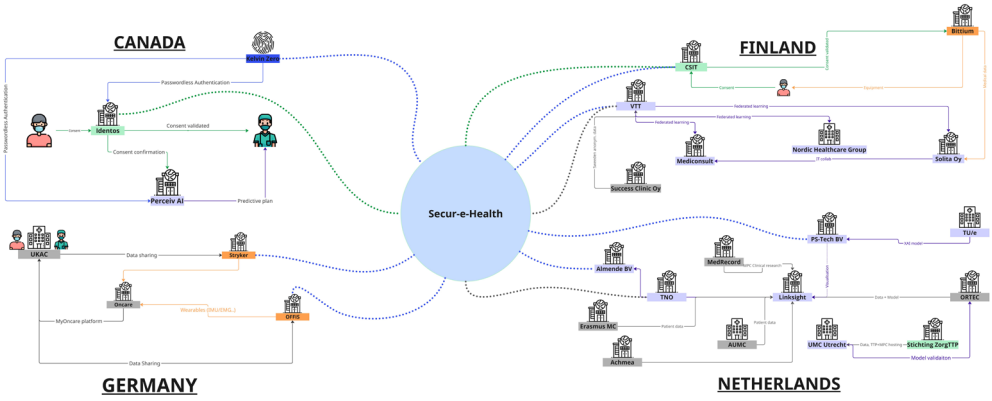
Healthcare costs are rising worldwide due to comorbidity and aging populations, placing strain on both practitioners and patients. Nevertheless, sensitive health data is often kept in silos due to fragmentation, privacy constraints, cybersecurity risks and limited interoperability, all of which negate the potential of such data for legitimate medical, research and analysis purposes. A new approach is needed that allows hospitals, service providers and research institutions to collaborate more effectively, thereby leading to improved predictive models, more efficient treatments, accelerated clinical research and, ultimately, better healthcare outcomes.

Project developments

Secur-e-Health aimed to address this challenge by empowering secure, interoperable digital healthcare ecosystems via federated data collaboration, privacy-by-design and trusted identities. This enables collaboration between healthcare institutions without moving or exposing sensitive patient data. From a business perspective, such an approach offers compliance-by-design, cross-border collaboration, reduced integration costs through standardisation, and faster clinical research and AI model development. For the wider healthcare system, this translates into benefits such as higher performance and reliability for AI-driven predictive models and increased efficiency in data-driven treatments, leading to improved overall healthcare quality and reduced economic burden.

Most hospitals are behind on cybersecurity but all could benefit from better medical equipment; convincing them to invest specifically in cybersecurity instead of equipment is therefore almost a non-starter. To remove the need to make such a decision, Secur-e-Health focused on enabling data use while maintaining secure data handling, developing a wealth of technologies for different phases of a patient's journey in healthcare. This could start, for instance, with the patient using the project's biometric cards and multi-pass authenticator for password-free login to the healthcare system. A mobile application could then act as a biometric smartcard reader for greater security or replace the biometric smartcard altogether for a more convenient, fully digital experience. When the patient arrives for their appointment, prediction models and federated learning then support the planning of the care pathway without moving data.

Those examples can be applied broadly, but Secur-e-Health also developed technologies according to specific conditions. For example, cardiovascular recovery can be assisted with electrocardiogram home monitoring and AI analysis, designed to give the patient full control over consent for the use of their data while providing researchers with verifiable evidence that this consent is compliant with strict GDPR requirements. For femur shaft fractures, conversely, a computer-assisted surgery (CAS) system has been developed to prevent revision surgeries and pain caused by incorrect fracture reduction. The system uses a security-by-design approach, ensuring sensitive information remains protected through encryption, anonymisation and secure access controls like two-factor authentication; it can also be connected to the aforementioned security card system, demonstrating how Secur-e-Health's innovations work both independently and in tandem.



Making the difference

These illustrative examples are the tip of the iceberg: across the consortium, Secur-e-Health developed twelve cross-organisation datasets, eleven products and services, seven systems and demonstrators, and two libraries for privacy-enhancing technologies (PET)

or federated learning components. With these technologies to securely unify different healthcare silos, users will be able to more easily conduct high-end medical research, thereby improving medical predictive model quality and data-driven treatment efficiency. Remarkable results have already been demonstrated on both counts: prediction model quality has been improved by 70% versus a target of 30%, while diagnosis and treatment accuracy has been increased by 50% against a target of 15%. In addition, cross-organisation computation and analysis time can be reduced by 50% per use case and the set-up time for digital ID systems has been brought down from 30 minutes to just two.

As such, these results have drawn strong interest, with 54 clients on trial at the project's conclusion and a further seven already converted to paying clients. The full list of results can be found in the dedicated Secur-e-Health Magazine, with exploitation highlights including FIDO2 validation and approval for Kelvin Zero's biometric card product KZero Passwordless, the first demonstration of Stryker's CAS system Femur LAR, and the enhancement of Linksight's data analytics platform with a governance hub for greater privacy in data collaborations. These examples demonstrate a strong foundation for rapid commercialisation, but open-source solutions are also critical: by making the PET libraries freely available in multiple programming languages, the project ensures that anyone can get started with privacy-enhancing technologies, helping to democratise access among the next generations of developers to enter the field.

Future outlook

Democratisation is a pertinent point considering the interest in AI in recent years. This has forced a reassessment of how data should be handled, especially as relying on a small number of American or Chinese providers to handle vast amounts of data is neither sustainable nor desirable. This opens the door to a renewed discussion on data sharing, including the need for countries to rethink regulation and move from discouraging sharing to enabling it securely. Given the possibility to extend many of Secur-e-Health's innovations beyond healthcare, such as in finance and pharma, the project thus hopes to be part of a shift towards safe, confidential data sharing on a level far beyond what exists today.

Major project outcomes

Dissemination

- 35+ publications, 30+ conference participations, 1 magazine, living LinkedIn page

Exploitation (so far) - See Secur-e-Health Magazine for more details

New products:

- Synthetic data generation engine
- Multi-Pass biometric smart card (FIDO2 certified)

New services:

- Sensor-data interface integrated into myoncare
- U-Prevent Connect for EHR-prepopulated CDS
- Multi-Pass Authentication Service

New systems:

- MDR-approved remote cardiac monitoring platform
- Computer-assisted surgery demonstrators

Standardisation

- **Cybersecurity and digital identity**: Contributions to baseline cybersecurity controls and digital credential standards, including FIDO2 validation for biometric NFC cards.
- **Interoperability and privacy**: Support for secure access, federated analytics, federated learning, and synthetic data as emerging de facto standards.
- **Healthcare data standards**: Implementation and tooling for HL7 v2 and HL7/FHIR, including FHIR libraries and OMOP dataset conversions.
- **Secure data exchange**: Deployment of secure infrastructure for trusted partner data sharing.

ITEA is the Eureka RD&I Cluster on software innovation, enabling a large international community of large industry, SMEs, start-ups, academia and customer organisations, to collaborate in funded projects that turn innovative ideas into new businesses, jobs, economic growth and benefits for society. ITEA is part of the Eureka Clusters Programme (ECP).

https://itea4.org

Secur-e-Health

20050

Partners

Canada

- IDENTOS
- Kelvin Zero
- Perceiv Research

Germany

- OFFIS
- Oncare
- Stryker Trauma
- University Hospital Aachen AöR

Finland

- Bittium Biosignals
- CSIT Finland
- MediConsult
- Nordic Healthcare Group
- Solita
- SUCCESS CLINIC
- VTT

The Netherlands

- Achmea
- Almende
- Amsterdam University Medical Center
- Eindhoven University of Technology
- Erasmus MC
- Linksight
- MEDrecord
- ORTEC
- PS-Tech
- Stichting ZorgTTP
- TNO
- UMC Utrecht

Portugal

- Fundação Fernando Pessoa
- Instituto Superior de Engenharia do Porto (ISEP)
- MTG Research & Development Lab
- University of Porto Faculty of Medicine

Project start - Project end

November 2021 - December 2025

Project leaders

Thierry St-Jacques-Gagnon, Kelvin Zero
Alexandre Peyrot, Kelvin Zero

Project email

tg@kzero.com
a.peyrot@kzero.com

Project website

https://itea4.org/project/secur-e-health.html