

Contents

[**Introduction** 3](#_Toc162096544)

[1 **Health technology landscape** 3](#_Toc162096545)

[1.1 **Breakdown of current technologies in healthcare** 3](#_Toc162096546)

[1.2 **Impact on patient care, efficiency, and accessibility** 4](#_Toc162096547)

[2 **Security measures and best practices** 5](#_Toc162096548)

[2.1 **Security challenges** 5](#_Toc162096549)

[2.2 **Secur-e-health’s key technologies** 6](#_Toc162096550)

[2.3 **Ethical considerations regarding patient data privacy** 10](#_Toc162096551)

[2.4 **Lack of interoperability and integration of technologies in the medical field** 11](#_Toc162096552)

[3 **Future outlook** 12](#_Toc162096553)

[3.1 **Predictions on the future of health technology and security with Secur-e-Health** 12](#_Toc162096554)

[3.2 **Potential challenges** 12](#_Toc162096555)

[**Conclusion** 13](#_Toc162096556)

[**The crucial role of Secur-e-Health in a data-driven healthcare future** 13](#_Toc162096557)

[4 References 15](#_Toc162096558)

# **Introduction**

The ever-changing realm of healthcare relies heavily on the dynamic interplay between technological progress and protection of confidential information. This intersection of health and data security is crucial, as it not only harbors potential for improved patient outcomes through innovation, but also necessitates a sturdy framework for privacy and confidentiality. The Secur‐e‐Health project emerges as a pioneering force, harnessing cutting-edge technologies such as artificial intelligence (AI), machine learning (ML), fully or adaptive homomorphic encryption (FHE/HE), federated learning (FL), Multi-Party Computing (MPC) and time dependant cox models to revolutionize the healthcare domain.

As the healthcare sector evolves, it is essential that we prioritize the integration of digital identity technologies and the implementation of privacy-preserving analysis methods. This is why the Secur-e-Health project is crucial in redefining the future of healthcare. By providing a secure system infrastructure, the project aims to promote collaboration among various international medical institutions. Through the seamless fusion of cutting-edge technologies, the project envisions a future where data-driven insights and analysis will lead to significant advancements in medical predictive models, treatment effectiveness, clinical research speed, and overall enhancement of healthcare delivery.

This document aims to delve into the current state of the healthcare ecosystem, outlining the challenges and opportunities that form the backdrop in which the Secur-e-Health project takes part of. By promoting a comprehensive understanding of the project's objectives in the current state of the healthcare world, we endeavor to elucidate its potential to shape a future where the intersection of health and data security is synonymous with unparalleled innovation and improved healthcare outcomes.

# **Health technology landscape**

## **Breakdown of current technologies in healthcare**

There are a growing number of technologies that are changing how we deliver, access, and manage healthcare for the patients all over the world. One such technology that hospitals increasingly rely on now is **Electronic Health Records (EHR)** systems. EHRs are the digitised platforms that help healthcare providers store and access healthcare information. EHR not only improves how we deliver care but also how we coordinate it.

**Telemedicine**, too, has expanded as a reaction to the global need for remote health care services, with video consultations, wearable monitors and apps connecting healthcare professionals with patients and enabling early interventions in a manner that reduces the burdens on healthcare institutions.

**AI and machine** **learning** are revolutionizing the healthcare industry, providing vital tools for diagnostics, personalized treatments, and predictive analytics. By analyzing enormous amounts of medical data, AI algorithms can uncover patterns, predict the progression of diseases, and even aid in drug discovery, ushering in a new age of precision medicine.

**Wearable devices**, such as fitness trackers and smartwatches, have become a common feature in our lives, giving individuals the ability to monitor their health in real-time. Through data on physical activity, sleep patterns, and vital signs, these devices enable proactive health management and preventive care, empowering individuals to take control of their well-being.

**Blockchain technology** has also found its way into the healthcare industry, providing a secure and efficient way to manage patient data and maintain the accuracy of medical records. Its decentralized nature ensures transparency, security, and compatibility of health information across various healthcare providers.

Furthermore, **the Internet of Things** (IoT) is playing a vital role in transforming traditional healthcare systems into smart hospitals. The integration of devices, sensors, and equipment enables real-time monitoring of data, streamlined workflows, and effective resource management, leading to enhanced efficiency in delivering healthcare services.

In summary, the current advancements in healthcare technologies highlight a dynamic and continuously evolving landscape. The emergence of digital health is just the beginning of a future where technology plays a significant role in improving the quality and accessibility of healthcare.

## **Impact on patient care, efficiency, and accessibility**

The integration of diverse technologies in healthcare is significantly transforming the landscape, resulting in profound impacts on patient care, efficiency, and accessibility.

Particularly when it comes to **patient care**, these technological advancements are leading to a revolutionary era of precision and personalized medicine. By leveraging Artificial Intelligence (AI) and machine learning, healthcare providers are able to analyze vast amounts of medical data to identify patterns and improve their decision-making processes. This facilitates the development of personalized treatment plans, catering to the specific needs and characteristics of each patient. Additionally, wearable devices and remote monitoring technologies facilitate continuous tracking of health metrics, offering real-time data for managing chronic conditions and enabling proactive, preventive care.

Technological advancements have significantly impacted **efficiency** in healthcare delivery, optimizing various processes. A prime example is the implementation of Electronic Health Records (EHRs), which digitize patient data and enhance communication among healthcare providers, while also minimizing errors linked to traditional paper-based records. Moreover, telemedicine has revolutionized the way patients and providers interact, saving valuable time and reducing strain on healthcare facilities. Virtual consultations are especially effective for routine check-ups and minor issues, leading to more streamlined and convenient healthcare experiences.

These innovative technologies are revolutionizing healthcare by promoting **accessibility**. As mentioned right above, patients can now utilize telemedicine to connect with healthcare professionals from any location, especially beneficial for those residing in remote areas or with limited mobility. Through the implementation of blockchain technology, medical data can be securely and seamlessly shared among providers globally, enhancing collaboration and maintaining consistency in care for patients with complex medical needs. Additionally, wearable devices are empowering individuals to actively engage in their health management, delivering instant updates on physical activity, sleep quality, and vital signs.

In summary, the current technologies in healthcare are reshaping the industry to be more patient-centric, efficient, and accessible. But while the integration of advanced technologies in healthcare brings about significant benefits, the increased digitization also raises concerns about the security of sensitive medical data. The potential vulnerabilities within these technological systems pose a considerable challenge, as the consequences of security breaches in healthcare can be severe and far-reaching.

# **Security measures and best practices**

## **Security challenges**

As we continue to see enormous strides in healthcare technology, the need to protect sensitive data has reached an unprecedented level. With the explosion of digital platforms and electronic medical records, safeguarding confidential patient information has emerged as a top priority. Not only does this help maintain the integrity of individuals' personal data, but it also plays a key role in upholding patient confidentiality and building trust.

**Electronic Health Records** (EHRs) are highly susceptible to cyber attacks due to the vast amount of patient information they store. Such unauthorized access not only violates patient privacy but also puts the accuracy of medical records at risk. Maintaining patient confidentiality is a pivotal ethical and legal responsibility in healthcare, and any compromise in security can undermine the trust between patients and the medical community.

The rise of **telemedicine** also presents a series of complex security concerns. With the transmission of sensitive health information over video consultations and remote monitoring systems, there is an increased risk of interception. As a result, securing telehealth platforms becomes imperative in order to safeguard patient data from unauthorized access during virtual appointments.

As the use of **Artificial Intelligence** (AI) and **machine learning** (ML) in healthcare continues to expand, there are important considerations to keep in mind. While these innovative technologies provide valuable tools for diagnostics and treatment, they are not without their vulnerabilities. Adversarial attacks, in which malicious actors manipulate input data to deceive AI systems, pose a significant security risk. Furthermore, the vast datasets used to train these powerful algorithms and models may contain sensitive patient information, raising concerns about potential privacy breaches if proper protection measures are not in place.

The utilization of **blockchain technology** holds great potential for ensuring the integrity of data, yet it does not come without its own obstacles. To effectively safeguard against unauthorized access and manipulation, smart contracts and distributed ledger systems must be built with strong security protocols. Smart contracts, which are self-executing code on the blockchain, can contain vulnerabilities that could compromise data security. Bugs or loopholes in smart contracts may be exploited by attackers to gain unauthorized access to sensitive information. Also, even though blockchain ensures data immutability, it does not protect against data leakage at the source. If sensitive information is inputted into the blockchain in an insecure manner, it can still be exposed to unauthorized parties.

To address all those potential threats, we have had to innovate in Secur-e-Health with our methods and technologies to become pioneers in preserving patient data confidentiality. By implementing the most robust security measures and staying ahead of emerging threats, we strive to ensure the highest level of privacy and protection for our patients' information.

## **Secur-e-health’s key technologies**

**Multi-Party Threshold cryptography (MPTC)**

Threshold cryptography and Multi-Party Threshold Cryptography (MPTC) computation is a realm of cryptography that stands as a paradigm to allows multiple parties to jointly compute a function over their inputs while allowing these inputs to remain private. As the National Institute of Standards and Technology (NIST) points out (National Institue for Standardization and Technology - NIST, 2021), “the multiparty paradigm of threshold cryptography enables a secure distribution of trust in the operation of cryptographic primitives. This can apply, for example, to the operations of key generation, signing, encryption and decryption”.

The allure of threshold cryptography and the multi-party paradigm lies in its promise to enable collaboration on sensitive data without sacrificing confidentiality all the while improving security. It presents vast potential across various domains such as secure confidential digital identity systems, privacy-preserving data analysis, secure distributed and isolated computations, blockchain or other cryptography-based technologies. Its distributed nature also plays well with decentralized approaches, providing greater, low-hanging, integration, and interoperability opportunities for its adopters.

Even though the early signs of threshold cryptography can be dated back to Adi Shamir’s Secret Sharing (Shamir, 1974) and that additional work was published De Santis and al. (De Santis, 1994), the adoption and standardization of such systems is still in its nascent stage. Recently, we observed a growing interest in these concepts through the user of blockchain technologies due to its cryptocurrency use cases, but also more recently with standardization efforts by NIST creating the first call for MPTC cryptographic schemes (National Institue for Standardization and Technology - NIST, 2024). This is also fueled by the ever-growing adoption of cloud-computing that offers tremendous advantages when it comes to scalable computing workloads but necessitate a trade-off on the privacy and exposure of data. Meanwhile, regulations often prohibit or restricts the possible exposure of sensitive data and renders the compliance difficult for organization looking to benefit from these advantages of the cloud. One approach has been to create special, segmented enclaves in the cloud, but this recreates the old problem of “data silos”. MPTC can offer a different approach that doesn’t not require a compromise between convenience of cloud and the privacy, security, and compliance aspects. Secur-e-Health is looking at the possibility of contributing to the MPTC standardization effort with schemes developed during the project and some organizations are in contact with NIST as well as their national cryptographic authority.

Ultimately, the MPTC developed in the context of Secur-e-Health can enable cross-border collaborations for researchers, worldwide, to analyze sensitive data, fostering global and optimized solutions to various challenges without compromising data sovereignty across borders. The potential of MPTC to revolutionize medical research is both profound and multifaceted and can be leveraged to overcome several longstanding challenges in medical research.

***Enhancing Privacy and Security***

One of the most significant barriers to collaborative medical research is the need to protect patient privacy and comply with stringent data protection regulations like HIPAA in the United States or GDPR in Europe. MPTC can enable researchers to perform analyses on combined datasets from multiple healthcare providers without any party having to reveal the data they hold. This means sensitive health records do not need to be centralized or exposed, drastically reducing the risk of data breaches while still allowing valuable insights to be extracted.

***Facilitating Cross-Institutional Studies***

Medical research often requires large, diverse datasets to ensure findings are robust and widely applicable. However, pooling data from multiple institutions is fraught with legal, ethical, and logistical challenges. MPTC offers a solution by allowing institutions to contribute to research studies without actually sharing their data. This could accelerate the pace of discovery by making it easier to study rare conditions, understand broader population health trends, and develop treatments tailored to specific demographics.

***Enabling Secure Access to medical Data***

Genomics and medical markers are fields of medical research with enormous potential but equally significant privacy concerns. MPTC can safeguard the privacy of individuals participating in genomic studies, for example, by allowing researchers to query genomic databases without revealing the genetic information of participants or the specifics of the query. This approach could open up vast genomic datasets for research that were previously too sensitive or regulated to access, speeding up the discovery of genetic markers for diseases and personalized medicine.

***Boosting the Development of Personalized Medicine***

Personalized medicine, which tailors medical treatment to the individual characteristics of each patient, relies heavily on data. MPTC can securely integrate diverse types of data (clinical records, genomics, wearables data) from various sources to create comprehensive patient profiles. By analyzing these profiles, researchers and clinicians can develop more effective, individualized treatment plans without compromising patient privacy.

***Overcoming Data Silos***

Medical data is often siloed within different departments of a single hospital or across various healthcare institutions, making it difficult to gain a holistic view of patient health or population trends. MPC allows for the secure analysis across these silos, facilitating a more integrated approach to medical research and healthcare provision. This integrated approach can lead to better disease prediction models, improved public health strategies, and a more cohesive understanding of health and disease.

While the potential is immense, realizing the full benefits in medical research requires overcoming several challenges. Current MPTC protocols can be computationally intensive, especially when the computation involves complex functions or many participants. It also remains a very complex expertise to acquire, touching mission critical components of computing. To address this, researchers are usually actively exploring one of the various avenues at the time:

* Optimized protocols:
	+ Designing MPTC protocols that are inherently more efficient, by reducing the amount of communication required between parties or the computational overhead.
* Hardware acceleration:
	+ Leveraging specialized hardware, such as GPUs, Hardware Security Modules (HSMs) or secure enclaves (e.g., Intel SGX), can significantly speed up the cryptographic computations underlying MPTC.
* Hybrid approaches:
	+ Combining MPTC with other cryptographic techniques, such as homomorphic encryption (HE) or Privacy Enhancing Technologies (PETs), such as Federated Learning or Cox as described later, or secure hardware, to create hybrid systems that offer a balance between performance and security.
* High-level programming language Libraries:
	+ Building libraries and APIs that abstract away the complexity of MPTC, enabling developers without deep cryptographic knowledge to integrate MPTC into their applications.
* Standardization Efforts:
	+ Efforts to standardize MPTC protocols and interfaces will facilitate interoperability and ease of use, like what has been achieved with SSL/TLS for secure web communications.
* Educational Resources:
	+ Increasing the availability of educational materials and resources to train developers and researchers in the nuances of MPTC can bridge the knowledge gap.

Secur-e-Health is taking a multi-prong stand, currently tackling all these avenues simultaneously while applying them to concrete healthcare technologies and medical research use cases. Additionally, we integrate MPTC with other technologies to create an even greater and safer approach to use medical data.

**Fully or additive Homomorphic Encryption (HE)**

Homomorphic encryption is a cryptographic technique enabling computations to be performed directly on encrypted data. Applied in the healthcare context, it ensures that confidentiality of health data is preserved while allowing for data analysis, data sharing, and collaboration among disparate healthcare systems. When combined to federated learning technique, one of the most compelling benefits of homomorphic encryption lies in its ability to facilitate secure and privacy-preserving collaborative research and analysis, aiming at achieving personalized healthcare aid and support. Between fully and additive homomorphic encryption, the used choice should be according to available system resources as well as required computation capabilities.

In the project, by implementing a system that encrypts data at the source and performs computation and learning in the encrypted domain, we facilitate creating new settings for healthcare organizations to overcome interoperability challenges and data silos, enabling data exchange and integration across healthcare platforms and stakeholders. In the long run, this interoperability-driven approach not only aims at streamlining clinical workflows but also empowering patients to securely access and share their health information across different care settings and providers, facilitating continuity of care and patient engagement. In addition, usage of homomorphic encryption helps to enforce privacy requirements of GDPR into healthcare data usage.

**Federated Learning (FL)**

With Federated Learning we refer to a protocol where multiple parties, that own sensitive or confidential data, collaborate to co-train a (machine learning) model without sharing their data, supported by a not-fully-trusted third party, usually referred to as server.

In this framework sensitive data never leave the local servers, while only the parameters of the model under training are iteratively communicated between the server and the parties according to the following schema:

1.      the central server communicates to all the parties an initial model;

2.      each party trains the received model using their local data and communicates back to the server the updated model parameters.

3.      the server aggregates the parameters sent by each party in a new model (for example by performing a weighted average) and communicate them to each party;

4.      points 2 and 3 are repeated either for a fixed number of iterations, or till when some other convergence condition is reached.

Federated learning algorithms can be split in two families, called horizontal and vertical federated learning, depending on how the data is distributed among the parties. Horizontal federated learning applies when different parties’ own similar information from a different set of individuals (e.g. different hospitals collecting the same medical information from different patients); vertical federated learning refer to the situation where different parties own different information about the same set of individuals (e.g. medical centers and health insurances, registering different data of the same set of people).

Federated learning can be considered a Privacy Enhancing Technology, since it improves the security of the input data, preventing sharing or central collecting of the data itself; anyhow depending on several factors (the data itself, the number of the parties, the complexity of the model), information could still be inferred from the shared parameters of the model. Those potential risks can be further mitigated by combining federated learning with other techniques, such as multi-party computation or other forms or differential privacy.

**Time dependent Cox models**

The Cox proportional hazards model (or simply Cox model) is a statistical technique used for survival analysis, i.e. to evaluate the effect of given variables (demographics, treatment regimens, biomarkers, …) on the probability that an (failure) event will happen in a certain moment.

The Cox model is a semi-parametric model, that assumes that the hazard (the risk of an event occurring at a given time) for any individual is a constant multiple of the hazard for any other individual, and that this proportionality holds over time.

This proportional hazard assumption can be relaxed, leading to the so-called time dependent Cox Models: those are more complex survival models where both the variables and the parameters of the model can be assumed to depend on time.

## **Ethical considerations regarding patient data privacy**

Ethical considerations regarding patient data privacy are paramount in the digital age of healthcare. Patients entrust sensitive medical information to healthcare providers, and concerns exist around the potential misuse of this data. These concerns include unauthorized access by hackers, breaches exposing sensitive data, and the use of anonymized data for commercial purposes without proper patient knowledge or consent. Additionally, the potential for algorithmic bias in healthcare AI models trained on such data raises concerns about discrimination in diagnosis or treatment.

This is where initiatives like Secur-e-Health become crucial. By prioritizing secure and interoperable data exchange, Secur-e-Health can help mitigate these ethical concerns. Here's how Secur-e-Health can contribute:

* Enhanced security protocols: The platform can enforce robust security measures to prevent data breaches and unauthorized access.
* Transparency and control: Secur-e-Health can provide patients with clear information about how their data is used and stored, empowering them with control over their information through features like granular consent options.
* Anonymization and pseudonymization: The platform can facilitate anonymized or pseudonymized data sharing for research purposes, minimizing privacy risks.

However, it is important to emphasize that the implementation of technical solutions alone is not enough to guarantee the confidentiality of patient data.

Indeed, the problem of interoperability of health technologies represents a major challenge. The lack of interoperability between systems and platforms makes it difficult to implement consistent and effective security and privacy measures.

Therefore, in the next paragraph, we will explore the challenges and solutions related to the interoperability of health data.

## **Lack of interoperability and integration of technologies in the medical field**

The medical field is undergoing a technological revolution, with the emergence of promising technologies such as multi-party computation, federated learning, homomorphic encryption, and Cox models. However, a major challenge remains: the lack of integration and interoperability between these technologies.

This lack of interoperability has negative consequences on several fronts. First and foremost, patients suffer. The difficulty of conducting studies with quality data leads to poorer treatment outcomes and limits access to personalized medicine. Additionally, ethnic bias in the available data exacerbates inequalities in access to care.

Medical research is also hampered by this lack of interoperability. Exploiting the full potential of data is compromised, slowing down the development of new treatments and increasing R&D costs. The healthcare system suffers, with lower efficiency, poor coordination between actors, and wasted resources.

The example of Covid-19 perfectly illustrates the dangers of this situation. The fragmentation of data hindered research on the virus, delaying the development of effective solutions. A larger, interoperable dataset would have allowed for faster results and saved lives.

Fortunately, a promising solution exists: the Secur-e-Health initiative. This project aims to develop a secure and interoperable platform for exchanging healthcare data.

By centralizing data, improving its quality, and making it accessible to different actors in a transparent and secure manner, Secur-e-Health has the potential to:

* Foster collaboration between researchers, doctors, and patients
* Optimize resource utilization
* Ultimately improve patient care

In conclusion, the lack of interoperability of medical technologies is a major challenge to overcome. The Secur-e-Health initiative offers a promising solution to create a more efficient and equitable healthcare system by fostering innovation and improving the quality of care.

# **Future outlook**

## **Predictions on the future of health technology and security with Secur-e-Health**

The healthcare landscape is undergoing a rapid transformation fueled by revolutionary technological advancements. Electronic health records (HER), telemedicine, AI & machine learning, wearable devices, blockchain technology and the internet of things (IoT) are disrupting traditional practices, opening new avenues for patient research, diagnosis, treatment, and monitoring.

However, this transformation is accompanied by significant challenges. The exponential growth in health data generated by patients and healthcare professionals poses critical issues of storage, analysis, security, and governance. The fragmentation of healthcare information systems (HIS) hinders smooth communication between healthcare players and limits access to patient data. Cybersecurity becomes a paramount concern with the increasing digitization of healthcare, as sensitive medical data is increasingly targeted by sophisticated cyberattacks. Finally, access to quality care remains a crucial challenge for many populations, particularly in underserved areas, perpetuating health disparities.

In the face of these challenges, new technologies and solutions are emerging to improve the quality, efficiency, and accessibility of healthcare. Artificial intelligence offers a wide range of applications, spanning from predictive diagnostics and personalized drug development to medical image analysis and administrative task automation. Robotics is increasingly employed for assisted surgery, rehabilitation, and telemedicine, enabling greater precision, risk reduction, and increased access to care. Biotechnology revolutionizes the treatment of chronic and rare diseases through innovative therapeutic solutions like gene and cell therapies. The Internet of Things (IoT) allows for real-time data collection on patient health, facilitating early monitoring and intervention in case of issues.

It is within this context that Secur-e-Health emerges, offering a platform for secure and interoperable healthcare data exchange. This platform aims to address the challenges of interoperability, security, and data access by leveraging cutting-edge technologies like multi-party computation (MPC), federated learning (FL), fully or additive homomorphic encryption (FHE/HE) and time-dependant cox models.

## **Potential challenges**

Looking towards the future, Secur-e-Health has the potential to revolutionize healthcare. However, the path to a fully optimized healthcare ecosystem built on this platform is not without obstacles. Widespread adoption by both patients and providers, robust data governance frameworks that address privacy concerns and ethical considerations, a sustainable funding model, and seamless integration with existing infrastructure are all crucial hurdles to overcome. Despite these challenges, the potential benefits of Secur-e-Health are undeniable. By working together to address these issues, stakeholders can pave the way for a more secure, efficient, and equitable healthcare system for all. In conclusion, Secur-e-Health represents a significant step towards a future where healthcare data empowers a brighter future for patients, research, and global health.

# **Conclusion**

## **The crucial role of Secur-e-Health in a data-driven healthcare future**

This document has explored the ever-evolving healthcare landscape, highlighting the dynamic interplay between technological advancements and data security. We introduced the Secur-e-Health project, a pioneering initiative harnessing cutting-edge technologies to revolutionize healthcare data exchange.

**The current healthcare ecosystem: A landscape of opportunity and challenge**

We examined the current state of healthcare technologies, showcasing a diverse range of innovations that are transforming patient care, efficiency, and accessibility. Electronic Health Records (EHRs), telemedicine, AI & machine learning, wearable devices, blockchain, and the Internet of Things (IoT) are all reshaping the industry. However, alongside these advancements lies the crucial challenge of data security. The ever-increasing volume of sensitive health data necessitates robust security measures to ensure patient privacy and trust.

**Secur-e-Health: A secure approach for the future**

Secur-e-Health emerges as a critical solution to address these data security challenges. By leveraging technologies like Multi-Party Computation (MPC), Homomorphic Encryption (HE), Federated Learning (FL) and time-dependent Cox models, the project aims to create a secure and interoperable approach for healthcare data usage. It has the potential to:

* **Enhance collaboration:** Facilitate collaboration between researchers, doctors, and patients, fostering innovation and accelerating medical progress.
* **Improve efficiency:** Streamline data exchange and analysis, leading to more efficient healthcare delivery and resource utilization.
* **Empower patients:** Provide patients with greater control over their data, fostering trust and engagement in their healthcare journey.
* **Advance research:** Enable secure, privacy-preserving research on vast datasets, leading to breakthroughs in personalized medicine and improved treatment outcomes.

**Challenges and the road ahead**

While Secur-e-Health offers a promising future, there are challenges to overcome. Widespread adoption by patients and providers, robust data governance frameworks, a sustainable funding model, and seamless integration with existing infrastructure are all crucial hurdles that require collaborative efforts from stakeholders.

**Conclusion: Secur-e-Health – A stepping stone to a brighter future**

Despite the challenges, Secur-e-Health represents a significant step towards a future where healthcare data is harnessed for the greater good. By prioritizing data security while unlocking the potential of data-driven healthcare, Secur-e-Health has the potential to transform the healthcare landscape, leading to a more secure, efficient, equitable, and ultimately, healthier future for all.

While digital identity and authentication, healthcare technologies and medical research are the key areas where Secur-e-Health focus, we envision the future where these developments will likely see its application across a broader spectrum of use cases such as:

* Internet of Things (IoT):
	+ In the IoT domain, MPTC can secure data aggregation from multiple devices without exposing individual data points, enabling privacy-preserving smart systems. This includes medical devices, something the consortium is also trying to integrate, if not for data analysis, at least for authentication of the devices;
* Financial systems;
* Military/Intelligence/Law Enforcement expanded collaborations and alliances within classified, confidential, or protected systems;
* Space exploration, Climate Change and Environmental Studies;
* Etc.

Secur-e-Health represents a paradigm shift in how medical research can be conducted in the era of big data. By providing a secure method for computing on sensitive data, it offers a path to overcome many of the privacy, security, and logistical challenges that currently hinder collaborative health research. As the technology matures and becomes more accessible, Secur-e-Health’s approach could play a central role in unlocking the next wave of medical breakthroughs, from understanding complex diseases to creating personalized treatment protocols, all while upholding the highest standards of privacy and data protection.

# References

*De Santis, A. a. (1994, 05). How to share a function securely. Retrieved from Association for Computing Machinery: https://dl.acm.org/doi/10.1145/195058.195405?ref=blog.threshold.network*

*Gong Q., Ruan H., Chen Y., Su X. CloudyFL: A cloudlet-based federated learning framework for sensing user*

 *behavior using wearable devices; Proceedings of the 6th International Workshop on Embedded and*

 *Mobile Deep Learning; Portland, OR, USA. 1–3 July 2022; New York, NY, USA: ACM; 2022. pp. 13–18.*

*National Institue for Standardization and Technology - NIST. (2021, 11 05). Multi-Party Threshold Cryptography MPTC. Retrieved from Computer Secruity Resource Center: https://csrc.nist.rip/Projects/threshold-cryptography#:~:text=Events%20Publications%20Presentations-,Overview,%2C%20signing%2C%20encryption%20and%20decryption.*

*National Institue for Standardization and Technology - NIST. (2024, 03). Multi-Party Threshold Cryptography MPTC. Retrieved from Computer Security Resource Center: https://csrc.nist.gov/projects/threshold-cryptography*

*National Library of Medicine (2023, 08) - A review of Privacy enhancement methodsfor Federated Learning*

 *in healthcare systems : https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10418741/*

*National Library of Medicine (2022, 07) - A novel Homomorphic approach for preserving privacy of patient*

 *Data in telemedicine : https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9228489/*

Olanrewaju R., Ali N., Khalifa O., Abd Manaf A. ICT in telemedicine: Conquering privacy and security issues

 in health care services. Electron. J. Comput. Sci. Inf. Technol. 2013;4:19–24

*Rieke N., Hancox J., Li W., Milletari F., Roth H.R., Albarqouni S., Bakas S., Galtier M.N., Landman B.A.,*

 *MaierHein K., et al. The future of digital health with federated learning.*NPJ Digit.

 Med. *2020;3:119.doi: 10.1038/s41746-020-00323-1.*

*Shamir, A. (1974, 11). How to Share a Secret. Retrieved from Massachussets Institute of Technology: https://web.mit.edu/6.857/OldStuff/Fall03/ref/ShamirHowToShareASecret.pdf?ref=blog.threshold.network*

*WHO. Ho K., Cordeiro J., Hoggan B., Lauscher H.N., Grajales F., Oliveira L., Polonijo A., Kay M., Santos J., et*

 *al.*Telemedicine: Opportunities and Developments in Member States. Report on the Second Global

 Survey on eHealth.*World Health Organization; Geneva, Switzerland: 2010*