Silvia Gabrielli, Sofia Piffer, Marco Bolpagni from FBK.

Human-Centered Design in LICORICE to enhance the adoption of Privacy-Preserving Solutions

In the evolving landscape of digital innovation, success is measured not only by technical sophistication but by how well people trust, understand, and adopt new technologies. The LICORICE Project embodies this principle, combining privacy-preserving technologies (PPTs) with secure identity management solutions across two ambitious pilot domains: a health pilot supporting respiratory disease patients and their clinicians, and a cyber threat intelligence (CTI) pilot designed to enable secure, privacy-conscious collaboration among organizations.

Yet, introducing privacy and identity technologies is only the first step. True innovation lies in making these technologies usable, understandable, and accepted. This is where human-centered design (HCD) becomes critical. LICORICE does not treat privacy and identity as mere technical components. Instead, it adopts a socio-technical perspective which integrates them with the lived realities of patients, clinicians, analysts, and cybersecurity professionals.

As the latest research in HCD of AI interaction suggests, true quality is found in the alignment between a system's capacity and the lived goals of its users. The LICORICE Project is built on this very principle, moving beyond "privacy-by-design" to embrace a "human-centered" model across our two application domains.

Bridging Technology and Human Experience

Privacy-preserving technologies such as federated learning, encrypted data exchange, and secure computation are often invisible to end users. They operate in the background, safeguarding sensitive information and enabling analytics without exposing personal data. While PPTs solutions work at macro level, secure identity management introduces another shift in perspective, this time more tangible for the end users. They give users control over digital credentials and the power to selectively disclose identity attributes. Together, these technologies promise greater levels of privacy and autonomy at both the micro and macro level of information governance.

However, without careful design, these innovations risk creating confusion or disengagement. A patient may not understand how a federated model protects their health data, or a cybersecurity analyst may be unsure how decentralized identity affects their access and responsibilities. The technologies themselves are not enough. The way users perceive, interact with, and trust them ultimately determines their success and final adoption.

LICORICE addresses this challenge through HCD, which anchors both PPTs and secure identity management technologies in real-world contexts. By involving users early, observing workflows, and iteratively refining interfaces, the project turns privacy protections from abstract concepts to meaningful features that people can understand and control. HCD acts as a bridge, connecting technical guarantees with human experience.

The Health Pilot: Empowering COPD/Asthma Patients and their clinicians

The LICORICE Health pilot demonstrates the potential, as well as the challenges, of integrating PPTs and secure identity management technologies in patient care. Patients living with chronic respiratory diseases rely on digital tools to monitor symptoms, track medication, communicate with clinicians, and receive predictive insights. These tools handle some of the most sensitive data imaginable: health status, lifestyle patterns, and biometrics. Protecting this information is critical, but so is making patients feel empowered rather than overwhelmed.

In this context, secure identity management plays a crucial role. Instead of being managed by a centralized provider, patient identity and consent are controlled directly by the individual through digital wallets. Patients can selectively disclose attributes, authorize data sharing for care or research, and retain control over their information. Privacy preserving analytics instead allow predictive models to benefit from aggregated data without exposing individual records. It is not enough for a digital wallet to be secure, it must feel synchronous and supportive rather than a source of "digital anxiety". By utilizing HCD to shape "decision moments," we help patients move from being passive subjects to active agents who understand their power to selectively disclose information. We are shifting the focus from the machine's output to the patient's perceived control and transparency, which are the true benchmarks of a high-quality interaction.

But as we anticipated, technical solutions alone cannot guarantee adoption. Patients vary in digital literacy, experience fatigue or anxiety, and may be concerned about stigma or discrimination. Here, HCD ensures that privacy and secure identity management are integrated into interfaces that are understandable, intuitive, and supportive. Through participatory workshops, iterative testing, and contextual observation, LICORICE explores how patients interact with consent mechanisms, credential wallets, and secure communication channels.

More than that, the project seeks to measure acceptance systematically. A custom evaluation scale is being developed to capture stakeholders' perceptions of control, trust, transparency, and willingness to use these tools over time. Clinicians' perspectives are also assessed, examining whether secure authentication and federated analytics fit smoothly into care workflows and enhance perceived clinical-legal safety. By combining design with measurement, LICORICE can provide evidence not only that these solutions work, but that patients and clinicians are willing and able to use them effectively.

The CTI Pilot: Trust and Privacy in Cybersecurity Collaboration

The project's second pilot operates in a very different, but no less sensitive, domain: cyber threat intelligence sharing. Organizations must collaborate to identify, analyze, and respond to security threats, yet sharing intelligence inherently carries risks. Sensitive information about infrastructure, vulnerabilities, or attack patterns could expose organizations if mismanaged. PPTs such as encrypted data exchange and controlled-access mechanisms protect this information, but success depends on trust and usability.

Secure identity management complements these mechanisms by enabling verifiable organizational identities. Analysts, SOC operators, and compliance officers can authenticate themselves, prove their roles, and selectively disclose information without exposing unnecessary organizational details. This decentralized approach reduces reliance on a single authority and strengthens confidence in collaborative networks.

Once again, the role of HCD is central. Analysts operate under pressure, requiring quick access to intelligence and clear interfaces that support rapid decision-making. Co-design methods and iterative testing ensure that secure authentication and privacy controls integrate seamlessly into existing workflows, minimizing friction and maximizing adoption.

LICORICE also measures acceptance systematically in the CTI pilot, exploring how trust, perceived confidentiality, usability, and operational efficiency influence willingness to participate in privacy-preserving intelligence sharing. Differentiated measures and evaluation scales will be used to capture the nuanced perspectives of multiple stakeholder groups, providing insights that extend beyond anecdotal observations.

HCD as the Integrative Layer

Across both pilots, HCD acts as an integrative layer between secure identity management and PPTs. It guarantees that the mechanics of decentralized identity, selective disclosure, federated analytics, and encrypted exchange are not isolated technical features but coherent, understandable, and trustworthy user experiences. Over the LICORICE evaluation phases, the deployment of HCD methods will help addressing questions such as:

- How can consent be linked intuitively to credential presentation?
- How do users perceive privacy preserving analytics without feeling exposed?
- How are control and transparency communicated consistently across interfaces?
- How do users perceive the benefits of secure identity management in daily practice?

By focusing on lived experience, HCD contributes to making PPTs as tools that users actually trust and adopt. Through structured measurement, the project can assess whether HCD interventions are effective, compare acceptance across pilot domains, and identify universal versus context-specific drivers of adoption. This research contributes to evidence-based guidelines for deploying privacy-preserving and secure identity management technologies in complex, sensitive environments, supporting Europe's broader goals of trustworthy digital innovation and digital sovereignty.

By merging advanced privacy technologies with a rigorous framework for interaction quality, we transform technical innovation into lasting societal value. We are charting a path toward a future where technology does not just process our data but empowers our lives through a dialogue built on autonomy, fairness, and mutual trust.

Building a European Model of Trustworthy Innovation

LICORICE demonstrates that privacy-preserving and secure identity management technologies cannot be designed in isolation from the people who use them. By embedding HCD throughout development and systematically measuring acceptance, the project ensures that innovations are technically robust, legally compliant, and socially meaningful.

In the Health pilot, patients gain agency over their data, clinicians integrate privacy seamlessly into care, and predictive analytics remain actionable and secure. In the CTI pilot, organizations can collaborate

confidently, authentication and identity verification are intuitive, and sensitive intelligence flows without compromising trust. Across both domains, HCD ensures that human experience drives design, adoption, and impact.

In LICORICE, an ethics-by-design perspective complements privacy-by-design by keeping technical and organisational choices aligned with fundamental rights and core ethical principles such as autonomy, fairness, accountability, and harm minimisation. From an HCD standpoint, this means translating these principles into human-centred requirements and decision criteria, for example: ensuring that privacy and identity-related processes remain understandable, that user agency is preserved, and that assumptions and potential unintended consequences are documented and revisited as the pilots evolve.

Trustworthy innovation also depends on solutions that are usable and understandable by diverse user groups, including people with different abilities, languages, levels of digital literacy, and situational constraints. LICORICE therefore treats accessibility and inclusion as cross-cutting quality attributes addressed through user-centred requirements, clear and consistent communication materials, and evaluation activities that consider cognitive load, and accessibility needs where applicable. By integrating these considerations early and iteratively, the project aims to reduce barriers to adoption and ensure that privacy-preserving and secure identity management capabilities remain comprehensible in real-world use.

Challenges and Planned Mitigations through HCD

Introducing privacy-preserving and secure identity management solutions into real-world settings raises challenges that are often human and organisational. Even robust safeguards can fall short if people do not understand what is happening, do not feel in control, or experience new processes as disruptive. In LICORICE, HCD is used to anticipate these barriers and support adoption through clarity, predictability, and trustworthiness in everyday use.

A first challenge is understandability: privacy-preserving mechanisms and decentralised identity concepts can be unfamiliar to non-specialists, leading to uncertainty or misinterpretation. Our planned mitigation is to elicit expectations early, identify points of confusion, and iteratively refine user-facing explanations and communication materials so that key actions and consequences remain clear.

A second challenge concerns trust calibration and perceived agency. In privacy-sensitive contexts, people need to understand what they are agreeing to, what is shared, and what the implications are, without turning decision-making into a burdensome routine. We plan to address this by focusing on critical “decision moments” in workflows, shaping them around meaningful choices and feedback, and assessing whether different stakeholder perspectives interpret these moments consistently.

A third challenge is workflow fit under real constraints, such as time pressure, interruptions, or varying levels of digital literacy. If a solution adds friction or shifts effort onto users, adoption will suffer. Our plan is to ground requirements in realistic tasks and contexts of use, iterate based on feedback, and evaluate whether the experience remains manageable across roles, settings, and levels of expertise.

Shaping the Future of Trustworthy Innovation

The journey toward true digital sovereignty is not one we can take in isolation. It requires a continuous, high-quality interaction between developers, healthcare providers, security experts, and citizens. As the LICORICE Project moves from the design phase into real-world deployment, we are gathering the empirical evidence needed to prove that privacy-preserving technologies can be as intuitive as they are secure. We invite you to be part of this co-orchestration of trust:

- *For Healthcare Innovators*: Explore our latest findings on how decentralized identity wallets can reduce patient anxiety and streamline clinical workflows without compromising sensitive biometric data.
- *For Cybersecurity Professionals*: Join our community of practice to see how federated analytics and encrypted exchange can be integrated into high-pressure SOC environments to foster more accountable collaboration.
- *For Researchers and Policymakers*: Access our emerging framework for measuring interaction quality, which provides a rigorous blueprint for aligning technical capacity with human values like autonomy and fairness.

By focusing on the lived experience of our users, we are making the next generation of European innovation not just technically robust, but socially meaningful. Together, we can ensure that privacy-by-design is always matched by trust-by-experience. In doing so, LICORICE is helping to chart the path toward a future where privacy, identity, and technology work together to empower people, strengthen institutions, and advance European innovation.