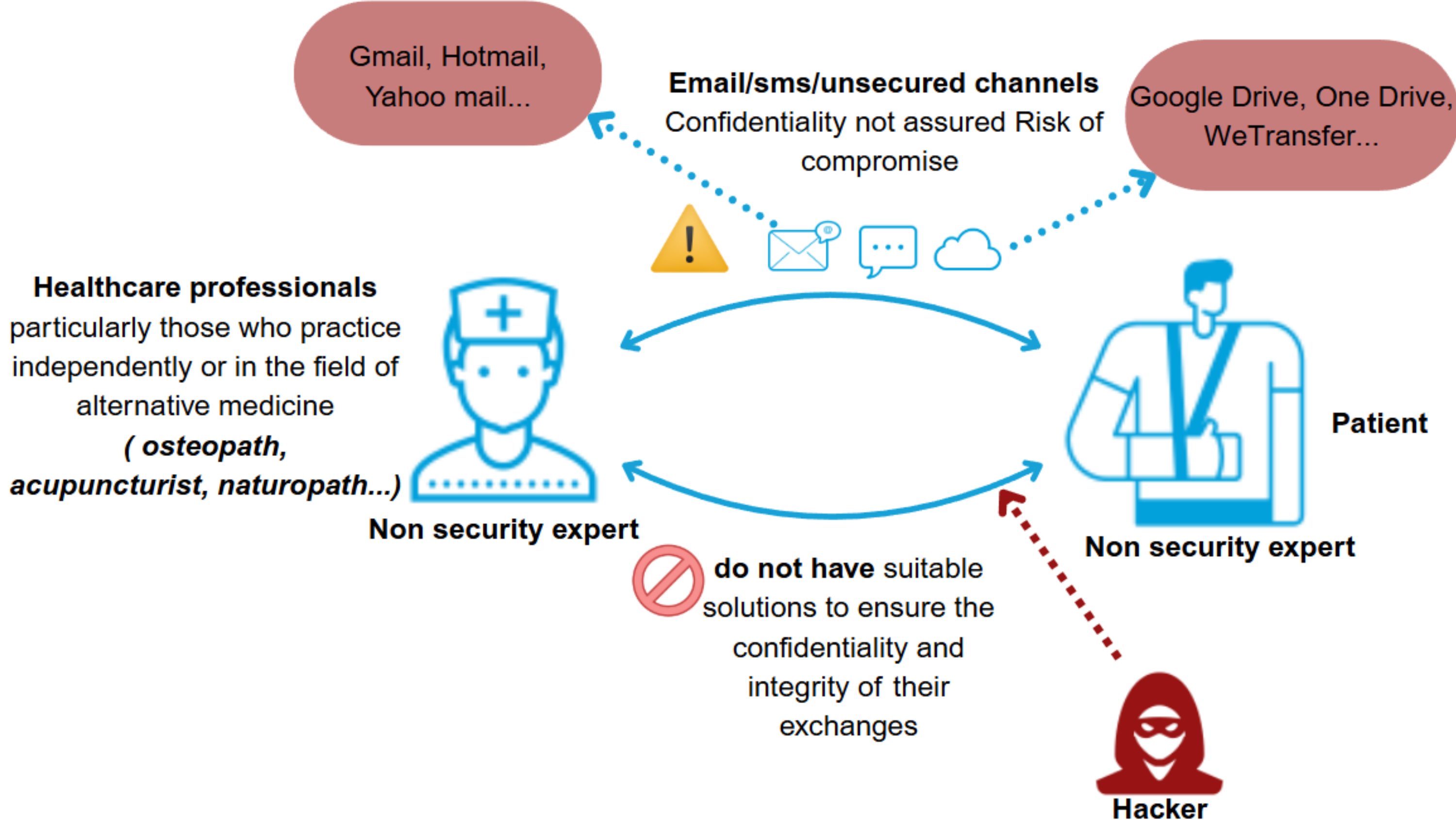


Meeting Healthcare Security Standards: From Legal Requirements to Technical Implementation

Ambre Journot, Karima Boudaoud, Christian Delette

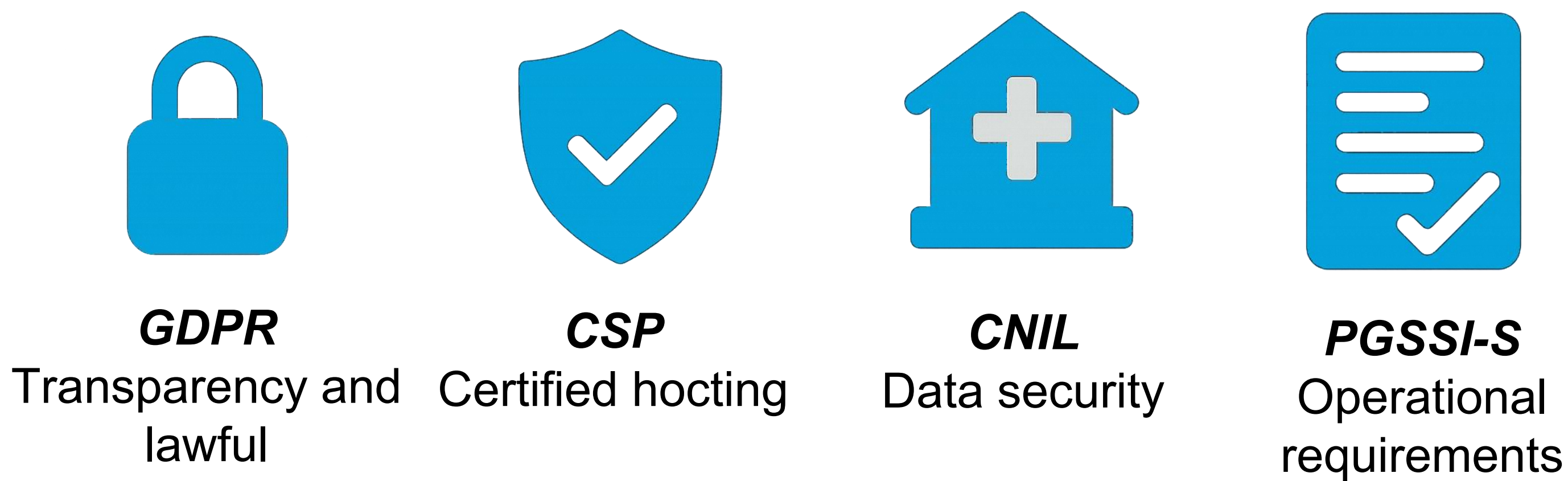


Problem Statement

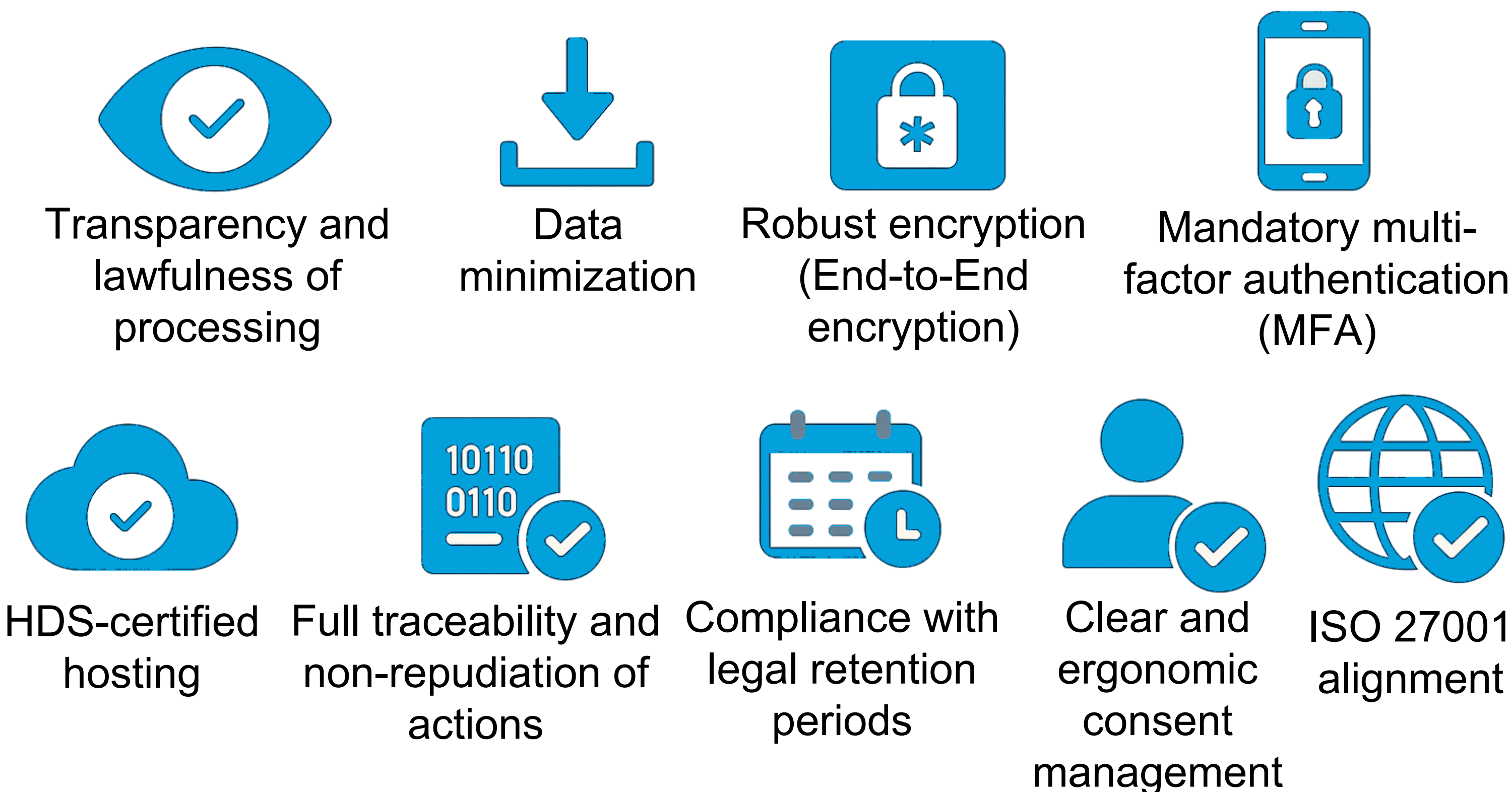


Solution/Requirements	ProtonMail	Signal	Session	Threema	MSSanté	IDOMED	FAST-Échange	Doctolib	U-HealthSec
Transparency and lawfulness of processing	No	Yes	Yes	Yes	Yes	Partial	Yes	Partial	Yes
Data minimization	Partial	Partial	Yes	Yes	Partial	Partial	Partial	Partial	Yes
Robust encryption (E2EE)	Yes	Yes	Yes	Yes	Partial	Partial	Partial	Partial	Yes
Mandatory multi-factor authentication	Partial	No	No	No	Partial	Yes	No	Yes	Yes
HDS-certified hosting	No	No	No	No	Yes	Yes	No	Yes	Yes
Full traceability and non-repudiation of actions	No	No	No	No	Partial	Partial	Yes	Partial	Yes
Compliance with legal retention periods	No	No	No	No	Yes	Yes	Partial	Yes	Yes
Clear and ergonomic management of user consent	No	No	No	No	Partial	Partial	Partial	Partial	Yes
ISO 27001	Yes	No	No	Yes	No	No	No	Yes	No

Legal Framework



Key Compliance and Security Criteria



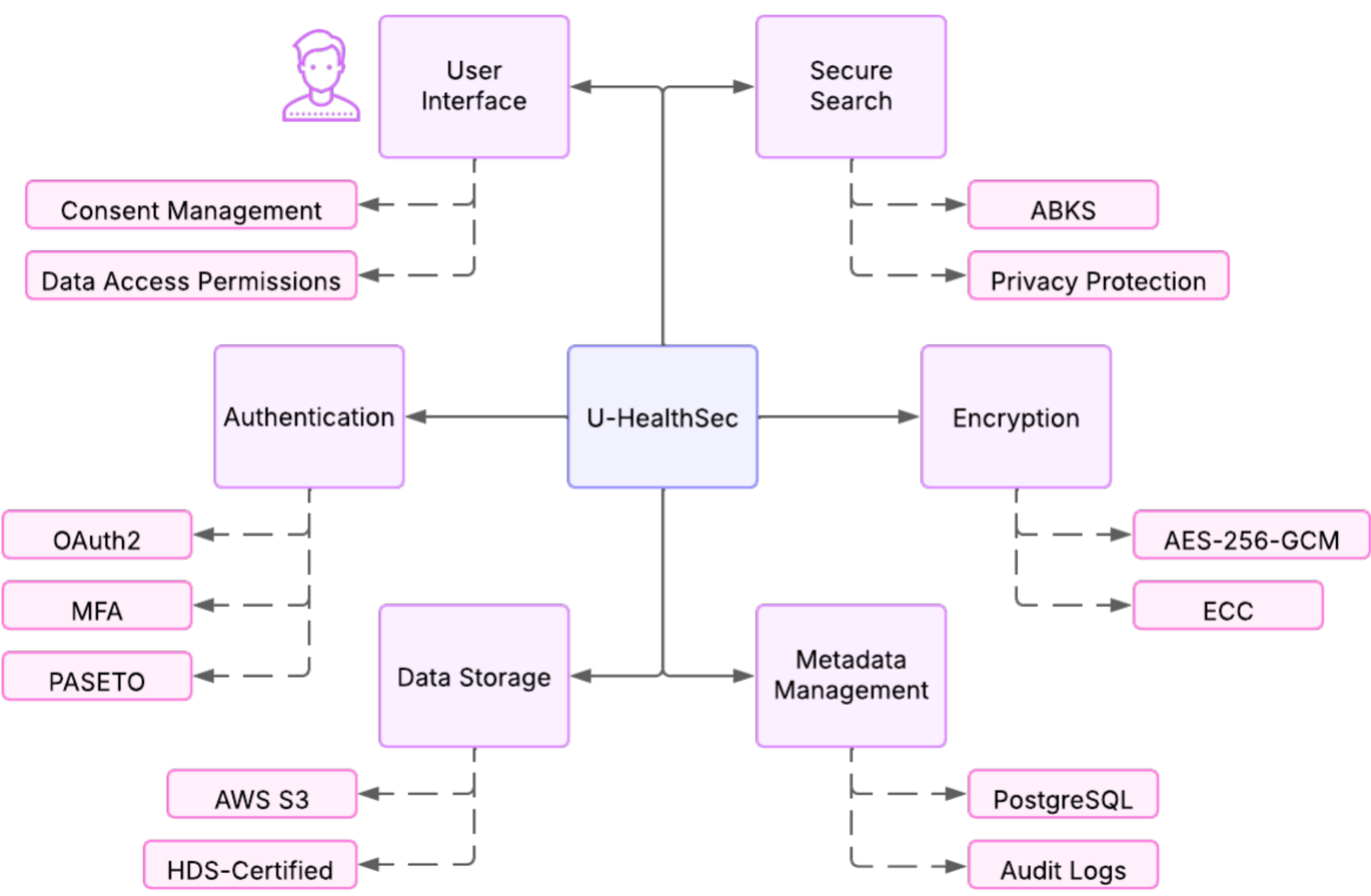
U-HealthSec

U-HealthSec is a privacy-by-design architecture developed to meet the stringent legal, technical, and usability requirements of healthcare professionals, particularly those practicing outside institutional infrastructures.

Key Components:

- Local Encryption (AES-256-GCM)
- Asymmetric Encryption (ECC)
- HDS-Compliant Storage

Comparison of existing solutions



U-HealthSec Architecture

- Secure Metadata Storage
- Strong Authentication (OAuth2 + MFA)
- Consent & Rights Interface
- ABKS Search

Key Advantages:

- Fully aligns with GDPR, CSP, CNIL, and PGSSI-S.
- Structured for future ISO 27001 certification.
- Modular and extensible for integration of advanced cryptography.

Conclusion

- Secure and compliant:** U-HealthSec addresses stringent healthcare data protection regulations (GDPR, CSP, CNIL, PGSSI-S).
- Robust architecture:** Integrates AES-256-GCM, ECC, MFA, and PASETO for end-to-end encryption and authentication.
- User-centric design:** Focus on intuitive consent management and accessibility for non-expert users.
- Traceability and privacy:** Ensures full logging, non-repudiation, and privacy-preserving search (ABKS).
- Future directions:** Exploration of advanced cryptographic techniques and mobile application support.



12th ACM Celebration of Women in Computing: womENCourage™
Braşov, Romania
17-19 September, 2025
Theme: Computer Science: a Catalyst for Educational Change

