Usable Security and Privacy for Connected Healthcare @ SOUPS

Connected healthcare systems increasingly rely on a diverse ecosystem of technologies, including Internet of Medical Things (IoMT) devices, remote monitoring platforms, patient portals, telehealth infrastructures, and AI-enabled health applications such as chatbots and clinical decision-support tools. These systems operate in safety-critical environments and handle highly sensitive data across complex workflows involving patients, caregivers, clinicians, and IT personnel.

Despite advances in security and privacy mechanisms, these controls often remain difficult to use, poorly aligned with clinical and home-care practices, or incompatible with regulatory and organizational constraints. This misalignment can lead to insecure workarounds, reduced trust, and, in some cases, patient harm.

This workshop aims to bring together researchers and practitioners working at the intersection of usable security, privacy, and connected healthcare. The goal is to examine domain-specific challenges, share emerging insights, and foster interdisciplinary collaboration. We particularly encourage contributions that engage with real-world contexts, user populations, and deployment constraints.

Topics of Interest

We invite submissions on human-centered security and privacy in connected healthcare contexts, including but not limited to:

- Usable privacy and security in IoMT and remote monitoring (home, clinical, or hybrid)
- User mental models, trust, and consent for AI-enabled health tools and chatbots
- Privacy-preserving interaction design for patient portals, EHRs, telehealth, and clinical decision support
- Authentication, access control, and delegation across patients, caregivers, clinicians, and administrators
- Balancing usability, safety, and regulatory requirements (e.g., HIPAA-aligned practices)
- Methods and metrics for evaluating usable security and privacy in healthcare
- Design patterns, anti-patterns, and guidelines for secure and privacy-preserving healthcare UX

Submission Types

We encourage two types of submissions:

- Full Papers (up to 8 pages, excluding references):
  Mature research contributions with well-developed methods, results, and implications.
- Position, Work-in-Progress, or Experience Papers (2–4 pages, excluding references):
  Early-stage research, design explorations, case studies, or perspectives intended to stimulate discussion.

Submissions should clearly articulate the context of use, user groups, and implications for design, practice, or policy.

Important Dates

- Submission deadline: June 1, 2026
- Author notification: June 11, 2026
- Workshop date: Co-located with SOUPS 2026 (Summer 2026)

Review and Participation

Submissions will be reviewed by the workshop Program Committee with an emphasis on:

- Relevance to usable security and privacy in healthcare
- Clarity of contribution and context
- Potential to stimulate discussion and interdisciplinary exchange

At least one author of each accepted submission is expected to attend the workshop and actively participate in discussions.

Accepted papers will be shared with participants prior to the workshop. We plan to produce a lightweight post-workshop summary (e.g., report or online document) capturing key insights, open challenges, and future research directions.

Workshop Format

The half-day workshop will include:

- Short presentations of accepted submissions
- Thematic breakout discussions (e.g., IoMT deployments, AI health tools, clinical workflows)
- A plenary session to synthesize insights and identify open research questions

Submission Details

- Submissions should follow the **SOUPS formatting guidelines**
- All submissions must be in PDF format and anonymization is optional.
- Submission Instructions: https://souphealthsec.web.illinois.edu/

Contact

For questions or inquiries, please contact the organizers:

- Prof. Masooda Bashir (University of Illinois Urbana-Champaign)
- Muhammad Hassan – mhassa42@illinois.edu (University of Illinois Urbana-Champaign)