IEEE/ACM CHASE 2026 WORKSHOP

mHealth Security Workshop 2026

Pittsburgh, Pennsylvania, USA | August 6, 2026 (tentative)

WORKSHOP OVERVIEW

The **mHealth Security Workshop** at IEEE/ACM CHASE 2026 provides a focused forum for researchers, practitioners, clinicians, and policymakers to discuss emerging threats, novel defenses, real-world deployments, and open challenges in securing mobile and connected health ecosystems. For more information: https://mhealthsecurity-at-chase.github.io/

TOPICS OF INTEREST

Topics of interest include, but are not limited to:

- Threat models, vulnerabilities, and risk assessment for mHealth apps, wearables, and remote monitoring systems
- Lightweight cryptography, secure communication, and key management for resource-constrained devices
- Privacy-preserving data collection and sharing
- Security and privacy of AI/ML models in mHealth (adversarial attacks, model stealing, robustness, secure training)
- Secure mobile sensing and behavior/physiological monitoring, including multimodal and wireless sensing
- Authentication, authorization, access control, and identity management for patients, clinicians, and devices
- Integration security between mHealth platforms, cloud services, IoT devices, and EHR systems
- Policy, regulation, compliance, and ethical considerations (HIPAA, GDPR, international frameworks)
- Security and privacy in telehealth, remote patient monitoring, and home-based care platforms
- Attack detection, anomaly detection, runtime monitoring, and incident response

IMPORTANT DATES

Paper submission deadline	**March 16, 2026**
Notification of acceptance	**April 7, 2026**
Camera-ready deadline	**April 20, 2026**

ORGANIZERS

Prof. Honggang Wang
Workshop General Chair (CHASE 2026)
Yeshiva University, USA

Prof. Yucheng Xie
Workshop TPC Chair
Yeshiva University, USA

Henry Ngo
Workshop Demo/Poster Chair
Yeshiva University, USA

Ashikur Nobel
Workshop Web Chair
Yeshiva University, USA

SUBMISSION GUIDELINES

Full Papers (Research/Experience)

Up to 6 pages (including references), describing original research, system design and evaluation, or significant deployment experiences and case studies.

Demo and Poster Abstracts

2-3 pages, describing tools, prototypes, datasets, or interactive systems relevant to mHealth security that can be showcased during the workshop.

All submissions must be in English and follow the main CHASE 2026 formatting guidelines (IEEE double-column format). Submitted papers must be neither previously published nor under review elsewhere. At least one author of each accepted paper must register for CHASE 2026 and present in person. Accepted papers will be included in the official CHASE 2026 workshop proceedings or companion volume, subject to conference publication policies.

Contact: Yucheng.xie@yu.edu
Conference Website: https://conferences.computer.org/chase2026/
Acknowledgment: The workshop is partly supported by NSF grant #2428595 (PI Wang).