

## Ethics Review Board Statement

Trustworthiness of ambient intelligence systems is critical to achieving the potential of this new technology. While there is increasing attention on trustworthy AI [14,15], we consider four separate dimensions of trustworthiness: privacy, fairness, transparency, and research ethics. Developing the technology while addressing all four factors requires close collaborations among experts from medicine, computer science, law, ethics, and public policy. PAC and HAI have brought together a committee of experts in these areas to assist in our projects.


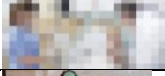

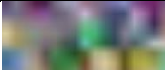

**Privacy:** Ambient sensors, by design, continuously observe the environment. Ambient intelligence can uncover new information about how human physical behaviors impact healthcare delivery. As citizens worldwide are becoming more sensitive to mass data collection, there are growing concerns over confidentiality, sharing, and retention of this information. It is, therefore, essential to co-develop this technology with privacy and security in mind, with the continued involvement of all stakeholders. Several emerging privacy-preserving techniques are presented in Table 1. We will work with critical stakeholders (patients, family, caregivers, etc.), legal experts, and policymakers to develop governance methods for ambient systems.

**Fairness:** Ambient intelligence will interact with different types of patient populations and the elderly, which compels us to scrutinize the fairness of ambient systems. Fairness is a complex and multi-faceted topic, discussed by multiple communities [16,17]. We focus on two aspects of algorithmic fairness: dataset bias and model performance, such as in our previous work [18].

**Transparency:** Our proposed ambient intelligence system can uncover insights into how healthcare delivery is impacted by human behavior. Clinicians and patients need to trust the findings before using them. Instead of opaque, black-box models, we believe the intelligent systems should provide interpretable results that are predictive, descriptive, and relevant. This can aid in the challenging task of acquiring stakeholder buy-in, as technical illiteracy and model opacity can stagnate efforts to deploy artificial intelligence in healthcare. Transparency is not limited to the algorithm. We would also take specific precautions for dataset transparency—a detailed timeline of how a dataset was designed, collected, and annotated.

**Research Ethics:** Ethical research encompasses topics such as scientific integrity, social responsibility, and protection of human subjects [19]. In our study, we will take informed consent and will perform an automatic de-identification of data (Table 1). We will consult with experts from law and ethics to determine appropriate steps for protecting all human participants, and the institutional review board will approve all research methods.

**Table 1. Computational approaches to protect privacy**

| Method                   | Description  | Hardware                          | Publications       | Example Output  |
|--------------------------|--|-----------------------------------|--------------------|---|
| Face Blurring            | Detects and blurs human faces  | Ambient sensor                    | Wang et al.[10]    |  |
| Dimensionality Reduction | Reduces the input complexity (e.g., low resolution, PCA)                               | Ambient sensor, edge computer     | Dai et al.[20]     |  |
| Body Masking             | Replaces people in videos with coarse, & faceless avatars                              | Edge computer                     | Kocabas et al.[11] |  |
| Differential Privacy     | Adds noise to individual data samples, minimally affecting population-level statistics | Edge computer                     | Xu et al.[12]      | N/A   |
| Federated Learning       | Learns from local data and sends incremental updates to a server                       | Edge computer, centralized server | McMahan et al.[21] |  |
| Homomorphic Encryption   | Data is encrypted, and computations are performed on encrypted data                    | Edge computer, centralized server | Acar et al.[13]    |  |