KetoLink: Connecting Health Data with Trust

Yu-Ting Chung
NetID: yc223, Email: yc223@rice.edu

Ya-Chuan Hsu
NetID: yh167, Email: yh167@rice.edu

Yu-Xin Lai
NetID: yl371, Email: yl371@rice.edu

Liang-Yu Chen
NetID: lc200, Email: lc200@rice.edu

***Abstract*—Abstract—This project enhances the KetoPilot mobile platform by introducing a graduate-level *Sharing + Privacy module* that empowers users to decide what to share, with whom, and for how long. Our system, called KetoLink, focuses on four integrated features—custom sharing profiles, an anonymous peer support community, time-limited sharing links, and a transparent privacy audit dashboard—implemented using Flutter and Firebase. Through these features, KetoLink demonstrates that human-centered privacy design and technical feasibility can coexist in a deployable mHealth system. The project not only extends the functionality of KetoPilot but also explores a broader question: how can design itself create digital trust?**

***Index Terms*—KetoPilot, Flutter, Firebase, data privacy, secure sharing, mHealth, user trust**

I. Introduction

As wearable and health-tracking technologies evolve, users generate large volumes of metabolic and behavioral data every day. Such data hold immense potential for medical research, preventive healthcare, and personal wellness, yet they also expose individuals to new privacy and ethical challenges. The same datasets that reveal progress toward a fitness goal may also disclose sensitive information about habits, diet, or even medical conditions.

Most health-tracking systems today treat privacy as an afterthought. They emphasize continuous data capture and cloud synchronization but rarely give users transparent, fine-grained control over their data flow. Users are often forced into a binary choice: either share everything or remain isolated.

The goal of this project is to bridge that gap. **KetoLink** extends the existing KetoPilot mobile platform with a modular *Sharing + Privacy layer* designed around the idea of "privacy as a feature." Rather than treating privacy as a restriction, KetoLink reframes it as a meaningful design element—one that fosters trust, social support, and ethical collaboration. Our approach focuses on usability, transparency, and lightweight security mechanisms suitable for real-time mobile contexts.

II. Project Motivation

KetoPilot provides an ideal foundation for this work. It already enables tracking of glucose, ketone, and GKI levels and supports personalized feedback through a clean Flutter interface. However, users currently have little control over how data are shared or visualized. From interviews with pilot users, three themes emerged: (1) users wanted to selectively share data with professionals or family members, (2) they wanted motivation from peers without exposing their identity, and (3) they wanted to verify when and how their data were accessed.

KetoLink aims to address all three challenges through four connected features that create an ethical, transparent, and human-centered data-sharing ecosystem.

III. Plan for This Project

Our design philosophy is modular: each feature can function independently but collectively forms a complete privacy-aware workflow.

A. Feature 1 – Custom Sharing Profiles

Objective: Provide granular yet intuitive control over data visibility.

Each user can create multiple sharing profiles—*Private*, *Doctor*, *Research*, and *Community*. A profile defines (a) which data metrics are shared, (b) the level of granularity, and (c) the expiration of access. Profiles are stored in Firestore as JSON documents and enforced locally before uploads. For example:

```
{ "profile": "Doctor",
  "metrics": ["glucose", "BHB"],
  "granularity": "daily_avg",
  "expires": "2025-12-31" }
```

This ensures that no sensitive data are transmitted beyond the user's consent. It also simplifies compliance with privacy frameworks such as GDPR or HIPAA for future extensions.

B. Feature 2 – Anonymous Peer Support Community

Objective: Enable safe, social interaction without compromising identity.

We will develop a community feed where users can share progress notes, photos, or motivational quotes. Each post is tagged with a randomized alias (e.g., "User#201") and stored with minimal metadata. Firestore's real-time streaming updates will allow instant refresh without centralized servers. To promote positive engagement, a sentiment detection model (via TensorFlow Lite) can analyze post tone locally on the device. This approach keeps computation private while demonstrating responsible AI integration.

C. Feature 3 – Time-Limited Sharing Links

Objective: Allow controlled collaboration between users and clinicians.

Through a single tap, a user can generate a read-only link to share recent summaries (e.g., one week of glucose data) with a

healthcare provider. Each link contains a secure token and an expiration timestamp, validated client-side before rendering. Once expired or manually revoked, the link becomes invalid. Reports are visualized as simple HTML dashboards hosted via Firebase Hosting, supporting real-time revocation and analytics logging.

D. Feature 4 – Privacy Audit Dashboard

Objective: Make privacy visible and measurable.

Every data access is logged with details including viewer type, time, and data scope. These events are rendered using Flutter's `fl_chart` package, producing line and bar charts that summarize access activity over time. Users can export logs for personal recordkeeping or compliance. This transforms privacy from a passive promise into an interactive, verifiable feature—giving users genuine confidence in their digital autonomy.

IV. System Design and Implementation

KetoLink's architecture consists of three tightly integrated layers:

- **Presentation Layer:** Flutter front-end for intuitive control, profile selection, and dashboard visualization.
- **Data Layer:** Firebase Firestore for structured documents and Firebase Storage for optional media.
- **Security Layer:** Firebase Authentication and JSON Web Token validation for secure, time-bound sharing.

Each layer communicates through clearly defined interfaces, allowing independent testing and flexible scaling. By emphasizing modularity, the design remains maintainable for small teams while ready for production-level deployment.

V. Evaluation and Expected Results

We will evaluate KetoLink across two key dimensions: technical performance and user perception.

From a system perspective, success metrics include:

- Data filtering latency below 400 ms per transaction.
- 99% accuracy of access logging verified via test scripts.
- Successful link expiration and revocation within 5 seconds.

From a human-centered standpoint, we will conduct short usability studies. Participants will be asked to perform simple tasks—such as switching profiles, posting anonymously, or generating a sharing link—and rate their clarity and confidence on a Likert scale. A score above 4/5 on "I feel in control of my data" will indicate success. Qualitative feedback will guide iterative UI refinements.

VI. Conclusion

KetoLink transforms KetoPilot from a personal tracker into a secure, social, and trustworthy health companion. By embedding privacy into each interaction, the system proves that ethical computing is both technically feasible and user-friendly. In the long term, this project lays groundwork for advanced extensions such as encrypted synchronization, federated data analysis, and adaptive privacy policies—paving the way for scalable, transparent, and responsible mHealth ecosystems.

VII. References

References

[1] MacroFactor, "Fastest Food Logger of 2025," 2025. [Online]. Available: https://macrofactorapp.com/fastest-food-logger-2025/

[2] Metabolic Mind, "THINK+SMART Program," 2025. [Online]. Available: https://www.metabolicmind.org/thinksmart/

[3] ELEC 491/591 Course Notes, "KetoPilot Feature Specification," Rice University, 2025.

[4] Google Flutter Team, "Flutter and Firebase Integration Guide," 2024. [Online]. Available: https://firebase.google.com/docs/flutter/setup

[5] A. Cavoukian, "Privacy by Design: The 7 Foundational Principles," Information and Privacy Commissioner of Ontario, 2011.