NeuroLock: Secure Storage Systems

By Group VIRUS
Riya Jain (GL) 2023441 | Sanskriti Gupta 2023487 | Shubhi Jain 2023517 | Satatya MT25084 | Yug 2023615
Usable Security and Privacy | IIIT Delhi

1. Introduction

1.1 Problem Statement

The management of psychiatric and mental health records in India continues to face significant challenges related to security, privacy, and accessibility. Most healthcare facilities still depend on fragmented, paper-based, or semi-digital record-keeping systems that are vulnerable to data loss, unauthorized access, and mismanagement. This lack of a standardized digital framework for psychiatric data handling leads to inefficiencies in clinical workflows and compromises patient confidentiality which is a critical concern in mental health settings where trust and privacy are paramount.

Additionally, the sensitivity of psychiatric data demands strict access control, yet many existing systems provide uniform access to all staff members, disregarding their professional roles and responsibilities. This absence of differentiated access leads to ethical issues and potential misuse of confidential patient information. The situation is further complicated by India's growing focus on digital healthcare transformation, where hospitals are rapidly digitizing records without implementing adequate data protection measures. Consequently, there is an increasing risk of privacy violations, data tampering, and non-compliance with evolving healthcare data protection norms.

1.2 Motivation

The motivation for this project stems from the urgent need to strengthen the security and privacy of psychiatric and mental health records. It is an area that remains highly vulnerable despite rapid digitalization in healthcare. In India, most mental health institutions still operate with limited digital infrastructure, and where electronic systems exist, they often lack robust security mechanisms. As hospitals transition toward digital record-keeping under initiatives like the Ayushman Bharat Digital Mission (ABDM), the absence of standardized safeguards exposes sensitive data to breaches and misuse.

Recent incidents underscore these vulnerabilities. In 2025, two major Delhi hospitals, Sant Parmanand Hospital and NKS Super Speciality Hospital reported server breaches that compromised patient records and disrupted operations. Similarly, the Star Health & Allied Insurance data leak (2024) exposed medical records and policyholder information on social media platforms, highlighting the weaknesses in health data management and protection in India. Such cases reveal that even large, established healthcare organizations remain ill-equipped to prevent or respond effectively to data breaches.

Globally, the 2020 Vastaamo psychotherapy data breach in Finland serves as a reminder of the devastating consequences of poor data protection in mental health. Hackers accessed and leaked thousands of psychotherapy session notes, later attempting to extort individual patients. The breach caused severe emotional distress, public outrage, and legal actions, becoming one of the most damaging mental health data incidents in history.

These examples illustrate the real and growing threat to sensitive mental health data, both in India and abroad. They emphasize that mental health records require the highest standards of confidentiality, authentication beyond what traditional healthcare IT systems currently offer. As India advances toward large-scale digital health ecosystems, the lack of secure and privacy-compliant platforms for psychiatric data management presents a critical gap. This project is motivated by the need to address this gap through a system that ensures confidentiality, accountability, and trust in digital mental healthcare.

1.3 Project Overview

The primary goal is to build an application that enables psychiatrists, therapists, psychologists, and administrative staff to safely access, update, and store patient records and therapy notes. The system will implement multi-factor authentication (MFA) using password, OTP (via email, SMS, or authenticator app), and optional biometric login for mobile devices, providing multiple layers of security. Records and notes will be encrypted, and all access activities will be logged for comprehensive auditing.

1.4 Target Users

The hospital staff groups who will utilize the system are:

1. Psychiatrists: Full access to patient medical and therapy history
2. Psychologists: Full access to both therapy notes and certain medical information, as appropriate to their role in patient care
3. Therapists: Access limited to therapy notes and session logs
4. Nurses: Access to medication prescriptions and schedules
5. Admins: Permissions to manage staff accounts and assign roles

1.5 Project Plan Structure

Phase 1: User Study & Requirements

Conducted user studies to capture workflows and requirements for all roles, including psychologists. Also considered students at IIITD as potential clients and patients. Produced detailed reports and design prototypes influenced by feedback from these groups.

Phase 2: Development & Testing
We will develop and test role-based dashboards and secure data storage for every user type, ensuring that psychologists have the appropriate access as per hospital policy. Will deliver the user guide and collect usability feedback from hospital psychologists, psychiatrists, therapists, and nurses.

1.6 Planned Features

Multi-factor authentication (MFA) for all staff including:

1. Username and password login
2. Second factor via OTP (email, SMS, or authenticator app)
3. Optional biometric login (fingerprint/FaceID) for mobile devices

Role-based access control (RBAC):

1. Psychiatrists: Full access to patient medical and therapy history
2. Psychologists: Access to therapy notes and medical data relevant to psychological care
3. Therapists: Therapy notes and session logs only
4. Nurses: Medication prescriptions and schedules
5. Admins: Staff account management and permissions

Secure therapy session notes module:

1. Entry and review of session notes for clinicians
2. Notes encrypted in the database
3. Auto-lock after inactivity, requiring re-authentication with MFA

Audit and activity logs:

1. Logging of every login attempt and record access
2. Alerts to admins for unauthorized or suspicious attempts

Adaptive MFA enforcement:

1. Low-risk access (like viewing appointments) needs just a login
2. High-risk actions (editing sensitive records) require re-authentication
3. Access from new devices or locations triggers additional verification

Secure file storage (optional add-on):

1. Upload and encrypt documents (lab reports, discharge summaries)
2. Access limited to authorized users with MFA

Mobile-ready deployment:

1. Executable Android APK for use on hospital tablets and phones
2. Data securely stored using backend VM/cloud databases, ensuring integrity and privacy
3. User-friendly role-based dashboards for quick access to key functions
4. Comprehensive usability studies and iterative design improvements before release based on staff feedback

2. User Research Methods

2.1 Primary Research Methods

1. Offline surveys targeting possible clients and people taking therapy. These collect direct feedback on usability needs and security expectations.
2. In-depth interviews with stakeholders such as psychiatrists, psychologists, nurses, and potential users, with transcripts for qualitative analysis.
3. Contextual interviews and role-play simulations (staff, patients, admins) to understand workflows and refine requirements based on actual hospital scenarios.
4. Usability peer reviews involving simulated users, focusing on validating wireframes and how actual workflows align with proposed designs.
5. Rapid prototyping and feedback cycles using low-fidelity wireframes, tested with real or simulated users.
6. Group and individual usability testing, with bug findings, screenshots, and feedback on functional and security aspects of the developed tool.

2.2 Secondary Research Methods

1. Literature review and analysis of published reports, academic papers, articles, and product documentation.
2. Case studies regarding psychiatric EHRs and MFA in healthcare.
3. Comparative analysis of competitor hospital apps to evaluate UI flows, existing MFA implementations, and security measures, informing improvements to the planned features.
4. Compilation of information from external sources to support trade-off analysis of different MFA and role-based access strategies in similar healthcare environments.

3. Primary Research - Surveys before making Lofi

3.1 Overview

Objective: To understand user perceptions, concerns, and preferences about mental-health apps, privacy, and therapy-seeking behavior before creating a low-fidelity prototype.

Target Group:
28 respondents
Students of IIIT-Delhi
Age: 18–24 years
Field: Computer Science
Education Level: Undergraduate

Survey Type:
Pre-LoFi, exploratory survey
Combination of multiple-choice, Likert scale (1–5), and open-ended questions
Focused on technology comfort, therapy attitudes, privacy concerns, trust in professionals, and app security features

Methodology: Respondents answered 21 structured questions and data was collected in Excel-ready format. Responses were anonymized and treated confidentially

3.2 Rationale for choosing the Target Audience

Even though the survey respondents are not the direct users of the proposed mental-health app (i.e., patients in a hospital), this group was selected for several reasons:

Tech-Savvy and Digitally Active: Students in this age group are highly familiar with apps, websites, and digital platforms. Their responses provide reliable insights on technology comfort, usability, and security preferences, which are critical for designing a user-friendly app.

Representative Early Feedback: As part of a pre-LoFi (low-fidelity) study, the goal is to explore general perceptions, concerns, and priorities regarding mental-health privacy. Students' feedback can reveal attitudes toward data security, privacy, and trust that are broadly applicable to potential app users.

Feasibility and Accessibility: University students are accessible for preliminary testing and quick data collection, enabling rapid iteration of the app design.

Proxy for General User Behavior: While they are not the exact target users, students' insights help identify pain points, desired security features, and privacy concerns, which can guide early app design decisions.

Foundation for Later Testing: Findings from this group will inform future surveys or LoFi tests with actual users (patients), ensuring that initial designs are technically sound, secure, and user-friendly before wider testing.

3.3 Key Questions

Demographics
Tech comfort — How comfortable are you using apps and websites?
Primary device(s) you use.
Have you ever considered therapy or counseling?
What factors made you hesitate or decide not to start?
How important would the privacy of mental-health records be in your decision to seek therapy in the future?
How concerned are you about personal data leaks in general (any kind, not just health)?
How much do you trust hospitals or clinics to keep digital health records safe?
What would worry you most if mental-health records were leaked?

What do you think is the main reason people avoid therapy?
How much do you trust mental-health professionals to keep conversations private (even offline)?
If you ever sought mental-health support, which setting would you prefer?
How sensitive do you think mental-health records are compared to other personal data?
How much do you trust hospitals or therapy apps to protect private mental-health information?
Which of the following worries you the most about using such an app?
Which security features would make you feel safer using such an app?
Who should legally own your mental-health data stored in a hospital app?
Please share any other concerns or suggestions regarding privacy and mental-health apps.

3.4 Raw Findings

Among the 28 surveyed respondents for the Pre-LoFi study on mental-health apps, all were undergraduate Computer Science students between ages 18 and 24, with a substantial male majority (21 out of 28). Technological comfort was very high, with nearly all rating themselves “very comfortable” or “comfortable” using technology, and smartphones being overwhelmingly the primary device of choice, followed by laptops/desktops.

Therapy consideration was relatively low; just 39% had ever considered therapy or counseling, and the main barriers to seeking it were social stigma, privacy and data-security concerns, cost, and lack of time. Privacy was consistently valued: 64% rated privacy of mental-health records as “extremely important” and 25% as “very important,” with concern about personal data leaks also running high. Concerns about privacy extended to institutional trust: very few respondents expressed high trust in hospitals or clinics to keep records safe, most clustered at the neutral or low-trust end of the scale, and nearly all declared that fear of privacy or data leaks was the number one reason people avoid seeking therapy. Job or insurance discrimination and identity theft were the most feared consequences of a data leak, while about one-fifth also worried about being judged or exposed to family.

Confidence in mental-health professionals to maintain confidentiality was also modest, again with most respondents expressing only moderate or low trust. When asked about settings, respondents split among in-person meetings (43%), no preference, and, to a much lesser extent, online or chat-based support. Most respondents considered mental-health data to be either less sensitive than or about as sensitive as banking information; only a small proportion thought it was more sensitive.

When evaluating digital security, users were sharply worried about risks: all respondents cited threats of data leaks and hacking when using mental-health apps; a quarter also mentioned staff misuse, and a few cited government or employer misuse. For security reassurance, the most valued features were multi-factor authentication, end-to-end encryption, biometric logins, regular security audits, and the ability to control who can view their records. Data ownership was very clear: 86% said the patient should legally own their records, with the rest favoring shared ownership, no one felt hospitals alone should own this data.

Finally, while only a handful wrote short comments, those who did reiterated these concerns: “security and privacy,” “authenticity and secure login,” and “privacy of data important.” This points to a user group that is tech-native and interested in digital mental health tools, but acutely sensitive to issues of privacy, risk, and user control, trust and safety features appear decisive for engagement with a mental-health app in a student setting.

Question	Average Score (out of 5)
Q5 – Tech comfort	4.54

Q9 – Importance of privacy	4.57
Q10 – Concern about data leaks	4.07
Q11 – Trust hospitals/clinics	2.54
Q14 – Trust professionals	2.89
Q17 – Trust hospitals/apps	2.54

4. Primary Research - Interviews before making Lofi

4.1 Overview

Objective: Identify user needs, preferences, and pain points from our direct stakeholders. Understand security and privacy expectations. Guide the design of a secure and user-friendly mental-health app accordingly. Consent was taken.
Interviews were around 20-30 minutes per person for deep understanding of the interviewee's mindset.

Target Group:
2 clinical + academic psychologists
1 Psychiatrist
1 Administrator
2 Medical Students learning psychology

Key Questions:
These varied per stakeholder given different requirements. General questions included their views on our idea and discussions over similar concepts. Everyone provided insights based on their past experiences in the field and their future expectations. Then there were person-specific questions like for admin (Do you believe you should have access to patient records or just the information about who has access to what and where?).

4.2 Raw Findings

Psychologist 1: He handles an average of 4–5 sessions per day, mostly one-on-one, with occasional group, family, or couple sessions. Patient referrals come from appointments, faculty recommendations, academic performance issues, plagiarism or conduct violations, and campus wellness teams. Currently, records are maintained manually, including basic identification data and session notes. Only the psychologist and psychiatrist involved with a patient have access to detailed notes, while patients can view appointment history and basic records. Administrative staff assist with logistics but do not access sensitive information.

"Confidentiality is crucial in mental health. Only the psychologist and psychiatrist involved should have access; patients can see basic history but not the detailed notes. Security is not just about storage, it's about who sees what."

Confidentiality is utmost, requiring strict role-based access for patient records. The planned digital portal will enhance efficiency, but it must maintain high security, potentially incorporating OTP or biometric authentication. Collaboration between psychologists and psychiatrists is selective, ensuring shared patients can coordinate treatment while other staff or professionals cannot access unrelated data. The portal will support desktops and laptops as primary access points, with mobile as a backup, maintaining security while facilitating administrative and clinical workflows.

Psychologist 2: She works internationally and relies on OneDrive for storing and sharing patient data. She reported that within her immediate team, confidentiality is not strictly enforced, and colleagues can access records freely for operational or collaborative purposes. According to her, confidentiality is considered necessary only for outsiders, such as people outside the organization or external auditors. This implies that internal workflows rely heavily on mutual trust and professional judgment rather than formal access restrictions. While this may facilitate collaboration and quick information sharing, it increases the risk of accidental exposure or misuse of sensitive patient information.

"Within my team, confidentiality doesn't really exist; everyone can access patient records. The focus is only on keeping data secure from outsiders; we trust each other with the information."

This perspective highlights the importance of implementing structured access controls, even within trusted teams, particularly for sensitive mental health data. While informal trust may expedite workflows and facilitate collaboration, a digital system with role-based permissions and activity logs would help protect patient privacy and maintain accountability. Cloud-based storage platforms like OneDrive can be convenient, but they require additional measures, such as encryption, secure sharing settings, and audit trails, to ensure compliance with confidentiality standards. Furthermore, this scenario illustrates a broader organizational challenge: balancing collaboration, efficiency, and strict data privacy in international or distributed teams.

Psychiatrist: He practices individually and currently maintains all patient records manually, including detailed notes on therapy and prescribed medications. Access is strictly limited to the psychiatrist, and patients can only know their appointments, but cannot see detailed records. Emergency situations or errors in manual record-keeping pose challenges, including difficulty in tracking historical data, sharing information with collaborating psychologists, and ensuring proper security. The lack of digital infrastructure makes record management time-consuming and prone to human error, underscoring the need for a secure and structured digital system to store, access, and update patient data efficiently.

"Currently, everything is on paper, and while I control access personally, it's cumbersome and risky. A digital system would make record-keeping more secure, organized, and easier to manage."

Manual record-keeping limits efficiency, collaboration, and scalability, especially for psychiatrists handling complex or long-term cases. Implementing a digital record management system would enhance the security, accessibility, and traceability of patient information, facilitate controlled access for collaborating professionals, and minimize errors associated with paper records. A well-designed digital platform would also help in tracking treatment history, managing prescriptions, and ensuring patient confidentiality, while supporting potential integration with hospital-wide systems in the future.

Medical Student 1: They described their experience with an EHR system called Orion at a hospital in Delhi. Orion stores patients' past health records, but medical students only have access to the data for patients they are assigned, without seeing the full patient history. They rely on the accuracy of patient-provided data and undergo months of training on privacy and security, particularly for high-risk patients, to ensure responsible handling of sensitive information. Key features of Orion include login authentication and department-wise categorization of patient records. The student emphasized the need for more accessible and uniform data for students, which would improve workflow while maintaining confidentiality. They highlighted the relevance of privacy in psychiatric cases, citing incidents where data leaks caused significant harm to patients' reputations and affected the hospital's credibility. Medical students are trained to empathize with patients and, as assistants to doctors, sometimes help manage notes under strict supervision.

"Every medical student is trained to handle patient data carefully. In psychiatry, even a small leak can ruin reputations, so privacy and empathy go hand in hand."

The interview highlights that structured training is essential for ensuring students handle sensitive psychiatric data responsibly. Role-based access in the EHR system allows students to assist doctors effectively without compromising confidentiality. Students value uniform and easily accessible records that improve workflow while maintaining security. Awareness of the high sensitivity of psychiatric records underscores the need for careful handling and strong ethical practices. Finally, collaboration with doctors shows the importance of balancing workflow efficiency with strict privacy protocols, ensuring both learning opportunities and patient trust are maintained.

Medical Student 2: The second medical student is in her first year of medical school and has limited exposure to clinical settings. She shared that her college still relies heavily on paper-based patient records, especially in psychiatry and outpatient departments. Students usually learn by observing doctors and keeping handwritten notes for academic purposes. There is a strong emphasis on maintaining confidentiality, but since everything is recorded on paper, it is often difficult to ensure privacy or prevent files from being misplaced. She believes a digital system could make record-keeping more organized and secure while helping students understand how to handle sensitive data responsibly.

“I have heard of cases when a high-profile patient’s data breach occured ruining not just his but the hospital’s reputation. So yes, I agree that this is an important issue.”

This student’s experience highlights the need for early medical training to include more practical exposure to digital health systems. While students are taught about privacy, they often lack practical experience in applying it in real-world record management. Her response highlights the need for introducing structured digital record systems early in medical education. Doing so would help students learn secure documentation practices, ensure continuity of care, and promote awareness of data privacy from the start of their careers.

5. Literature Review

5.1 Executive Summary

This comprehensive literature review examines academic papers that focus on usable security within healthcare information systems, with a particular emphasis on psychiatric and mental health applications. The analysis offers critical insights into striking a balance between security requirements and user-centered design principles, thereby creating systems that are both secure and practical for use by healthcare workers.

The healthcare industry faces unique challenges in implementing security measures that protect sensitive patient information while maintaining workflow efficiency and user acceptance. This literature review synthesizes findings from multiple studies examining usable security approaches in healthcare settings, ranging from multi-factor authentication systems to electronic health record interfaces and psychiatric facility design.

5.2 Authentication Methods

A clear preference is noted for hardware-based authentication solutions over traditional password systems. Suleski et al. (2023) found that healthcare workers strongly favor FIDO2 and WebAuthn technologies combined with physical security keys like YubiKeys, which significantly reduce phishing attacks while being more user-friendly than mobile-based one-time passwords.

Ahmadian et al. (2021) provided compelling evidence that simple educational interventions can dramatically improve security behaviors, with auto-lock system usage increasing from 38% to 93% following poster-based education campaigns. This suggests that user resistance often stems from lack of awareness rather than fundamental usability issues.

5.3 Interface Design and Error Prevention

The most significant quantitative findings emerged from studies of electronic medical record (EMR) interfaces. Zahabi et al. (2015) conducted a systematic review of 50 studies, revealing that copy-paste functions in EMRs cause 71% time duplication and significant data entry errors. However, implementing color-coding systems to distinguish between copied and original content, and adding patient identifier watermarks, can effectively prevent wrong-patient errors.

Buivydaite & Reen (2022) demonstrated through mixed-methods research with 71 clinicians that auto-population features reduced task completion time by 40.9%, while visual workflow dashboards improved navigation efficiency. Template reduction decreased data duplication by 71.4%, highlighting how thoughtful interface design can simultaneously improve security and usability.

5.4 Information Management and Privacy

Observed innovative approaches to balancing privacy requirements with operational needs. Dvoskin et al. (2002) described how architectural design in psychiatric facilities can achieve both patient privacy and staff safety through single-occupancy rooms with central observation points and indoor-outdoor dayrooms that provide patient choice without compromising security.

Rizwan et al. (2023) found that 81.4% of survey respondents accepted psychiatric hospital information systems when designed with patient-controlled access permissions, addressing the primary concern about sharing traumatic experiences repeatedly with different healthcare providers.

5.5 System Integration and Workflow

Cloud-based systems emerged as a preferred solution for healthcare organizations, with Rizwan et al. reporting potential cost reductions of 70% compared to on-premise solutions. The research consistently shows that systems succeeding in healthcare environments are those that integrate seamlessly with existing workflows rather than requiring significant process changes.

Elhai & Frueh (2016) provided practical guidance for mental health providers, demonstrating how encrypted messaging applications, VPN services, and secure communication tools can be implemented with minimal workflow disruption while maintaining HIPAA compliance.

5.6 User Training and Adoption

The literature emphasizes that technical security measures fail without appropriate user education and support. Ahmadian et al. showed that educational interventions using simple visual materials could reduce confidential file storage on desktop systems by 65% within seven months.

However, the research also identifies significant barriers to adoption, including digital literacy gaps among older healthcare workers and cultural resistance to electronic systems in developing countries like Pakistan.

5.7 Cost-Effectiveness and Scalability

Economic considerations prove crucial for healthcare security implementations. It is suggested that hardware-based authentication tokens, despite higher upfront costs, provide better long-term value through reduced support requirements and improved user compliance compared to software-only solutions.

Cloud-based architectures offer particular advantages for resource-constrained healthcare organizations, enabling sophisticated security features without requiring extensive on-site technical infrastructure.

5.8 Critical Analysis and Limitations

Strengths

There is empirical evidence for effective security approaches in healthcare, with several studies demonstrating quantifiable improvements in user performance and security outcomes. The diversity of methodologies, from systematic reviews to controlled interventions to architectural case studies, strengthens the overall evidence base.

Limitations

Most studies focus on developed country contexts, which may limit their applicability to resource-constrained healthcare systems. Additionally, long-term sustainability and maintenance costs of proposed solutions receive limited attention in the literature.

The psychiatric healthcare focus of several papers, while providing valuable specialized insights, may not fully represent broader healthcare security challenges in other medical specialties.

5.9 References

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. Journal of Healthcare Informatics Research. https://doi.org/10.1007/s10916-022-01832-0

Zahabi, M., Kaber, D. B., & Swangnetr Neubert, M. (2015). Usability and safety in electronic medical records interface design: A review of recent literature and guideline formulation. Human Factors: The Journal of the Human Factors and Ergonomics Society, 57(2), 227–256. https://doi.org/10.1177/0018720815576827

Buivydaite, R., & Reen, G. (2022). Usability of electronic health record systems in mental health care: A mixed-methods study. Journal of Medical Systems, 46(1), Article 50. https://doi.org/10.1007/s10916-022-01832-0

Elhai, J. D., & Frueh, B. C. (2016). Security of electronic mental health communication and record-keeping in the digital age. Journal of Clinical Psychiatry, 77(2), 262–269.

Dvoskin, J. A., Radomski, S. J., Bennett, C., Olin, J. A., Hawkins, R. L., Dotson, L. A., & Drewnicky, I. N. (2002). Architectural design of a secure forensic state psychiatric hospital. Behavioral Sciences & the Law, 20(4), 481–493. https://doi.org/10.1002/bsl.506

Ahmadian, L., Raeesi, A., & Abbasi, R. (2021). Confidentiality of information stored on the desktop of computers in a psychiatric hospital before and after an intervention. Journal of Hospital Administration, 10(2), 948–954.

Rizwan, M., Arshad, S., Aijaz, H., Shamim, M. F., & Munir, M. W. (2023). Implementation of hospital information system in psychiatry: A study in Karachi. Journal of Applied Engineering Technology, 7(1), 37–47.

6. Case Study: EHRs in Psychiatric Hospitals in India

6.1 Introduction

India is moving fast towards digital healthcare through the Ayushman Bharat Digital Mission (ABDM). Every citizen is expected to have a digital health ID and the ability to store and share their health records online. A key example is the Ayushman Bharat Health Account (ABHA) app. While this app shows great potential, a government-led case study found that it is often confusing for users. Issues such as difficult onboarding, technical terms (e.g., "ABHA address"), and unclear login steps reduce trust and adoption (UX4G ABHA Case Study, 2023). For psychiatric hospitals, where records contain highly sensitive details such as therapy notes and mental health assessments, these usability and trust challenges become even more critical.

6.2 Trust, Privacy, and Patient Perceptions

Trust is the backbone of digital health adoption. A scoping review of global studies reveals that individuals are more likely to agree to share health data when they have a clear understanding of how it will be used and protected (Papadopoulos et al., 2024).

In India, awareness of mental health is still low compared to other nations. Apart from that, digitalisation in the healthcare sector has not been fully implemented yet. A mixed-methods study in Northern India reported that only 37% of urban residents had heard of digital health IDs, and even fewer understood the benefits of these IDs. About 58% of respondents expressed concerns about privacy and misuse of their health data (Kaur et al., 2023).

For psychiatric patients and clients, these fears are crucial to understand, as it is still taboo to seek mental well-being. Thus, any data leak could lead to stigma or discrimination. This demonstrates that our system must obtain precise consent for data, clearly explain who can view what, and provide patients with the control to withdraw access when they wish.

6.3 Workflow Integration and Localization

For doctors and staff, a tool that can't be used in daily routines will be an issue. A pilot by NITI Aayog tested a digital decision-support system in Uttar Pradesh and found that while the technology was strong, adoption improved by only 25% after it was adapted to local workflows, when the application was translated into local languages, and simplified for frontline staff (NITI Aayog, 2022).

In psychiatric hospitals, psychiatrists are busy with diagnoses, nurses manage medication schedules, and therapists focus on detailed counseling notes. A useful system must therefore allow fast note-taking, easy medication logs, and local language options. Offline access is also important, as many Indian hospitals frequently experience internet issues. Without these, even the most secure EHR system risks rejection by staff.

6.4 Security and Access Control

Security must be a crucial point of psychiatric EHRs. Reports on global digital health adoption indicate that hospitals and patients require role-based access controls, where each type of staff member only sees what they need (Deloitte, 2021). For example, psychiatrists may have access to all records, while therapists only view session notes, nurses only see prescriptions, and administrators only manage accounts. In India, 64% of patients surveyed supported stronger authentication, such as OTPs or two-factor login, especially when sensitive records are viewed (Kaur et al., 2023).

This means a web app should use adaptive MFA: a normal login for routine tasks, but a second authentication step for sensitive actions, such as editing therapy notes or downloading records. This balance ensures data security without significantly slowing down daily workflows.

6.5 Encryption and Data Protection

From a technical side, the strongest safeguard is encryption. All patient data should be encrypted both during storage and when shared. Highly sensitive data, such as psychotherapy notes, should be protected with an additional layer of encryption to prevent unauthorized access, including that of IT staff, without proper clearance. The ABHA case study demonstrates that simply adding security is insufficient; patients and staff also require clear communication about how their data is being protected (UX4G ABHA Case Study, 2023). Similarly, the global trust review stresses that showing patients who accessed their data and when can directly increase their confidence in the system. In fact, 72% of patients in surveyed groups said audit logs would improve their trust in digital health systems (Papadopoulos et al., 2024).

6.6 Governance and Policy Alignment

Technology alone cannot ensure the safekeeping of psychiatric records. The NITI Aayog pilot found that without proper training, staff struggled to use new systems (NITI Aayog, 2022). In psychiatric care, where stigma and sensitivity are high, governance becomes even more important. Hospitals must train staff on confidentiality, set penalties for misuse, and align with India's ABDM standards for interoperability. At the same time, stricter consent policies are needed for mental health data, ensuring that patients' most private notes are not automatically shared with larger health databases. Embedding patient rights, such as consent withdrawal, access logs, and grievance redressal, will help create trust and long-term adoption.

6.7 Conclusion

A secure psychiatric hospital web app in India must combine usability, trust, and security. Usability lessons from ABHA emphasize the importance of simple onboarding and locally adapted workflows. Trust requires transparency, patient empowerment, and stronger consent. Security must include adaptive MFA, role-based access, and encryption. Ultimately, governance and training ensure that the system operates effectively in practice. If these are addressed together, psychiatric EHRs can provide Indian hospitals with a secure, reliable, and trustworthy platform for digital mental healthcare.

6.8 References

UX4G. (2023). Case Study: ABHA App – Ayushman Bharat Health Account. Government of India. Retrieved from https://www.ux4g.gov.in/case-studies/ux4g-abha.php
NITI Aayog. (2022). Healthcare AI Catalyst (HAIC) Report. Government of India. Retrieved from https://www.niti.gov.in/sites/default/files/2023-02/HAICReportNITIAayog.pdf
Deloitte. (2021). Digital Health Technology: Global Case Studies and Insights. Deloitte Insights. Retrieved from https://www.deloitte.com/us/en/insights/industry/health-care/digital-health-technology.html
Papadopoulos, I., Koulouglioti, C., Ali, S., & Lazzarino, R. (2024). Public trust and health data sharing: A scoping review. Health Education Journal, 83(1), 3–20. doi:10.1177/00178969221138483
Kaur, H., Singh, R., & Sharma, V. (2023). Perceptions towards electronic health records and uptake of digital health IDs among urban residents in Northern India: A mixed-methods study. Indian Journal of Medical Research. Retrieved from https://ijmr.org.in/perception-towards-electronic-health-records-uptake-of-digital-health-ids-among-the-urban-residents-in-northern-india-a-mixed-methods-study
https://www.ux4g.gov.in/case-studies/ux4g-abha.php
https://www.niti.gov.in/sites/default/files/2023-02/HAICReportNITIAayog.pdf
https://www.deloitte.com/us/en/insights/industry/health-care/digital-health-technology.html
https://journals.sagepub.com/doi/10.1177/00178969221138483
https://pmc.ncbi.nlm.nih.gov/articles/PMC4142510
https://ijmr.org.in/perception-towards-electronic-health-records-uptake-of-digital-health-ids-among-the-urban-residents-in-northern-india-a-mixed-methods-study
https://ijcrr.com/abstract.php?article_id=3332

7. MFA methods in Hospitals, including tradeoffs

7.1 Current State of MFA Adoption in Healthcare

Healthcare organizations lag behind other industries in MFA adoption, with only 56% adoption rate compared to 87% in the technology sector and 77% in insurance. Government healthcare facilities show even lower adoption at 48%, often due to legacy system constraints and regulatory complexity. Key adoption barriers in healthcare include legacy system integration challenges (cited by 87.3% of organizations), cost concerns averaging $142,800 for compliance assessments. Also workflow disruption fears among clinical staff and digital literacy gaps, particularly among older clinicians.

7.2 OTP Authentication in Hospital Settings

7.2.1 SMS-Based OTP Systems

Advantages include:

1. Low Implementation Cost: Minimal infrastructure requirements beyond existing mobile devices
2. Universal Compatibility: Works with any SMS-capable phone without app installation
3. Rapid Deployment: Can be implemented across hospital systems within weeks
4. Familiar User Experience: Most healthcare workers already understand SMS messaging

Disadvantages include:

1. Cellular Dependency: Requires reliable cellular coverage throughout hospital facilities
2. Security Vulnerabilities: SMS interception risks, especially in dense hospital environments
3. Delivery Delays: Network congestion can delay critical authentication during emergencies
4. Cost Accumulation: Ongoing SMS charges scale with user base (typically $0.02-0.05 per message)

In psychiatric settings, SMS-based OTP presents unique challenges like patient privacy concerns with phone number collection, staff working in secure units may have limited cellular access and emergency situations requiring rapid authentication cannot afford SMS delays

7.2.2 Email-Based OTP Systems

Advantages include:

1. Infrastructure Leverage: Utilizes existing hospital email systems
2. No Recurring Costs: After initial setup, no per-message charges
3. Rich Content: Can include institutional branding and security reminders
4. Audit Trail: Email systems provide comprehensive logging for compliance

Disadvantages include:

1. Email System Dependency: Single point of failure if email infrastructure experiences issues
2. Slower Access: Requires email client access, adding authentication steps
3. Spam Filtering: Hospital security systems may delay or block automated emails
4. Mobile Limitations: Email access on hospital-provided mobile devices often restricted

In psychiatric settings, SMS-based OTP presents unique challenges like patient privacy concerns with phone number collection, staff working in secure units may have limited cellular access and emergency situations requiring rapid authentication cannot afford SMS delays

7.2.3 Authenticator App-Based OTP

Advantages include:

1. Offline Capability: Works without network connectivity using time-based algorithms
2. Enhanced Security: Reduced interception risk compared to SMS
3. Multiple Account Support: A Single app handles multiple hospital system authentications
4. Cost Efficiency: No per-authentication charges after initial deployment

Disadvantages include:

1. App Installation Barriers: Hospital IT policies often restrict app installations
2. Device Management: Requires ongoing management of app installations and updates
3. Learning Curve: Healthcare staff require training on the authenticator app usage
4. Recovery Complexity: Lost or broken devices require manual recovery processes

Healthcare workers prefer physical security keys over mobile OTP solutions, with YubiKeys preferred by 73% of surveyed clinicians due to reduced cognitive load and faster authentication times.

7.3 Biometric Authentication Using Mobile Devices

Biometric authentication using native smartphone features, such as fingerprint or facial recognition, is increasingly favored in healthcare digital platforms. This method is swift; taking as little as one to two seconds and leverages familiar, built-in phone capabilities for clinicians already using modern devices. For psychiatrists and staff, biometric login minimizes password fatigue and can be well integrated into mobile-first workflows. However, biometry is not universally suitable. Some users may be uncomfortable sharing biometric data, especially in mental health contexts where privacy concerns are heightened. Technical hiccups also arise: frequent hand sanitization or gloves can interfere with fingerprint sensors; facial recognition can struggle in varied lighting or with PPE. Not all staff or patients own compatible devices, and for shared tablets or phones, biometric login cannot differentiate multiple users. For those who can and want to use it, biometric authentication often results in high user satisfaction and adherence, but apps must always offer alternative pathways for users unable or unwilling to provide biometric data.

7.4 Adaptive and Risk-Based Digital MFA

Adaptive risk-based multi-factor authentication (MFA) offers the best security-to-convenience ratio for digital-only psychiatric records. Rather than enforcing static rules on all users and actions, these systems analyze contextual information such as device type, location, login time, existing behavioral patterns, and recent access history to determine when extra verification is truly needed. For example, a clinician logging in from a known mobile device during a regular shift may only be prompted for fingerprint or app-based approval, while a first-time login from a new location or device, or attempts to access especially sensitive data (such as a full therapy record or controlled medication list), might require OTP or another step.

Such systems are highly compatible with mobile psychiatric platforms and considerably reduce login fatigue and workflow interruptions. They also adapt to emergencies, allowing swift access for crisis interventions when justified by context. However, adaptive MFA is complex to configure and maintain, requires robust data sharing between the app backend and security engine, and must be transparently communicated to users so they understand and accept variable authentication steps. When configured well, it substantially increases both actual and perceived security without disturbing clinical focus.

7.5 Security, Privacy, and Regulatory Factors

Digital psychiatric applications face unique expectations for data privacy and compliance, particularly given the stigma and personal nature of mental health records. OTPs, biometrics, and adaptive MFA all face different regulatory interpretations, but any robust implementation requires strong encryption, audit trails, and HIPAA (or relevant local jurisdiction) compliance. Mobile device management is essential, particularly as clinicians often use personal devices, creating risks if devices are lost, stolen, or used by family members. For psychiatric patient portals, user-controlled permissions and clear, accessible explanations of how to report access issues or suspected breaches increase trust and ethical transparency.

Achieving balance between urgent clinical access and rigorous privacy protection is especially challenging in psychiatry: adaptive tools that allow for graded responses (faster access for in-person staff during emergencies, heightened checks for remote or out-of-hours queries) are essential. Ultimately, regulatory adherence and security good practice must be designed into the digital platform’s core, not retrofitted, and should be reviewed continuously as both threats and regulations evolve.

7.6 Workflow Integration and User Experience

The usability and workflow impact of MFA options is critical in psychiatric contexts, where every moment spent on authentication is a moment less spent with a vulnerable patient. OTP methods add typing and waiting, and staff often report frustration or skip steps under pressure, especially during emergencies. Biometric techniques alleviate some of this load but aren’t feasible in all conditions, and fallback methods (like backup codes or security questions) should never rely on memory or physical tokens.

Adaptive MFA excels at invisibly protecting workflows, reducing interruptions for familiar patterns while increasing scrutiny where warranted. Analytics show improved staff satisfaction and a marked reduction in failed logins when adaptive or biometric-first strategies are used in busy clinical environments. However, a universal FAQ and help resource, regular training refreshers, and responsive technical support are essential, since psychiatric settings often employ diverse staff with widely varying comfort with digital tools. Customization options, like selecting preferred MFA methods or setting up "emergency bypass" roles for clinical leads, can further align security needs with optimal care delivery.

8. Competitive Analysis

8.1 Feature Comparison

Epic: A leading and comprehensive hospital EHR system offering strong clinical workflows, customizable modules, and integration with third-party tools; widely used in large healthcare networks.

Athenahealth: Cloud-based EHR solution focused on streamlined clinical and billing tasks, with robust security and flexible access for outpatient and specialty practices.

Cerner: Enterprise-grade EHR known for deep interoperability, powerful analytics, and adaptable modules for large hospitals and health systems, including behavioral health.

SimplePractice: User-friendly EHR designed for solo and small-group therapists, offering scheduling, notes, telehealth, and basic security features in a web/mobile app.

TherapyNotes: Specializes in mental health practice management for therapists and counselors, featuring templates, session notes, billing, and compliance tools.

System	MFA Options	Adaptive MFA	Biometric Login	RBAC	Encrypted Notes	Auto-lock & Re-auth	Real-time Alerts	Secure File Storage
Epic	Yes	Partial	Partial	Yes	Yes	No	Yes	Yes
Athenahealth	Yes	No	No	Yes	Yes	No	Yes	Yes
Cerner	Yes	Yes	Partial	Yes	Yes	No	Yes	Yes
SimplePractice	Yes (basic)	No	Yes	Limited	Yes	No	Basic	Yes
TherapyNotes	Yes	No	No	Yes	Yes	No	Yes	Yes

NeuroLock	**Yes (strong)**	**Yes (fine)**	**Yes (mobile)**	**Yes (granular)**	**Yes (per-note)**	**Yes (sensitive)**	**Yes (real-time)**	**Yes (RBAC+MFA)**

8.2 Insights

Most current systems offer MFA, RBAC, basic encryption, and file storage. But very few have fine-grained adaptive MFA, auto-lock/re-auth on clinical modules, or real-time, in-context alerts. NeuroLock adds unique depth with auto-lock MFA for session notes, per-note encryption, and administrator controls tailored for psychiatric workflows.

8.3 References

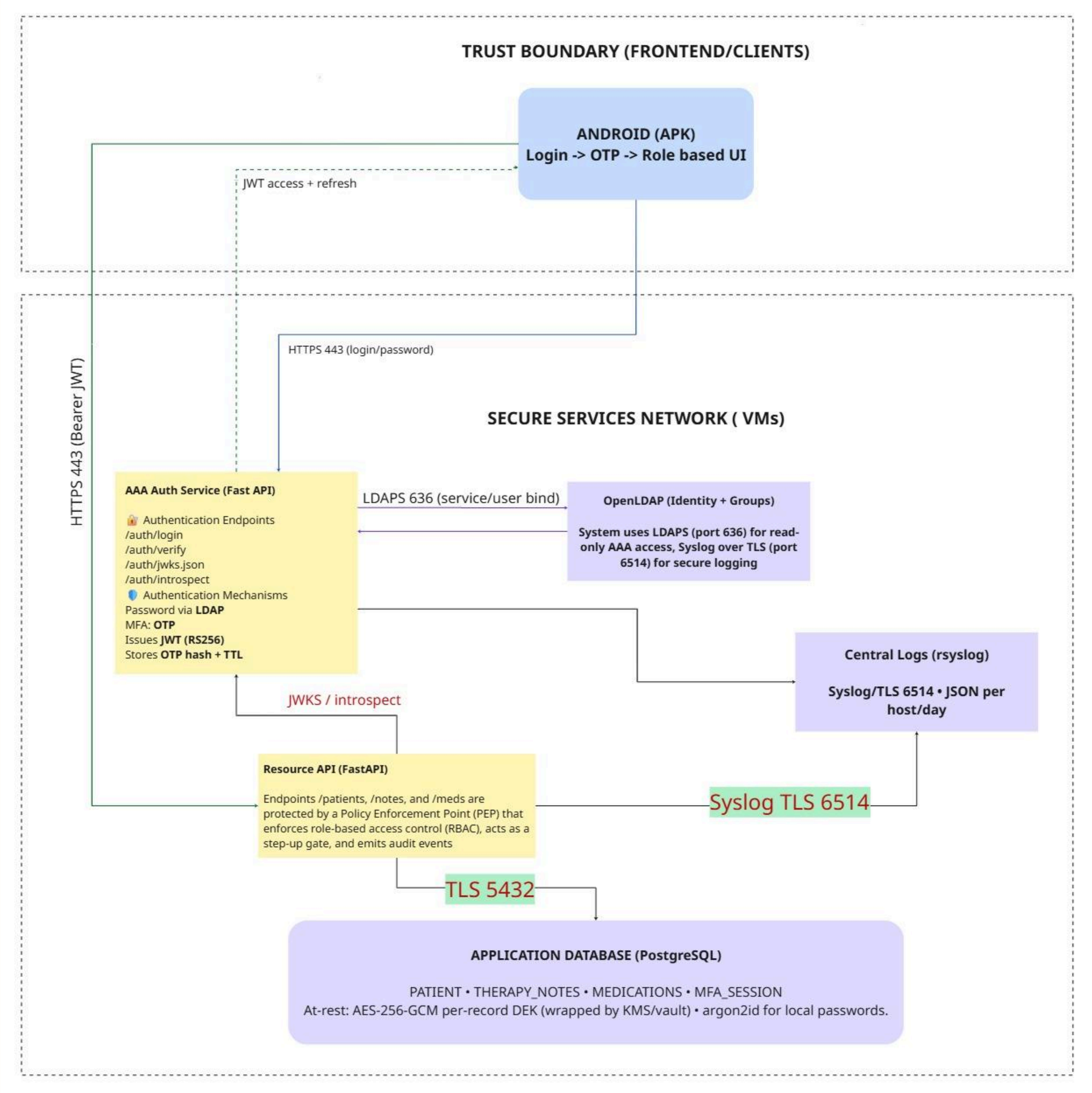
https://www.ehrinpractice.com/ehr-product-comparison.html
https://www.doctorsapp.in/blog/best-ai-driven-emr-for-psychiatrist-hospitals-in-india-2025
https://www.doctorsapp.in/blog/best-emr-for-psychiatrists-in-india-2025-top-10-psychiatry-emr-software-compared
https://omnimd.com/blog/top-mental-health-ehr-software-comparison/
https://www.choosingtherapy.com/best-mental-health-ehr/
https://www.medesk.net/en/blog/ehr-psychiatry/
https://www.psychiatry-cloud.com/blog/best-psychiatry-emrs-2025/
https://neklo.com/blog/best-ehr-software
https://www.softwareworld.co/mental-health-software/comparison/
https://www.remedly.com/why-mental-health-providers-are-choosing-remedly-in-2025/

9. System Design (Diagrams and Architecture)

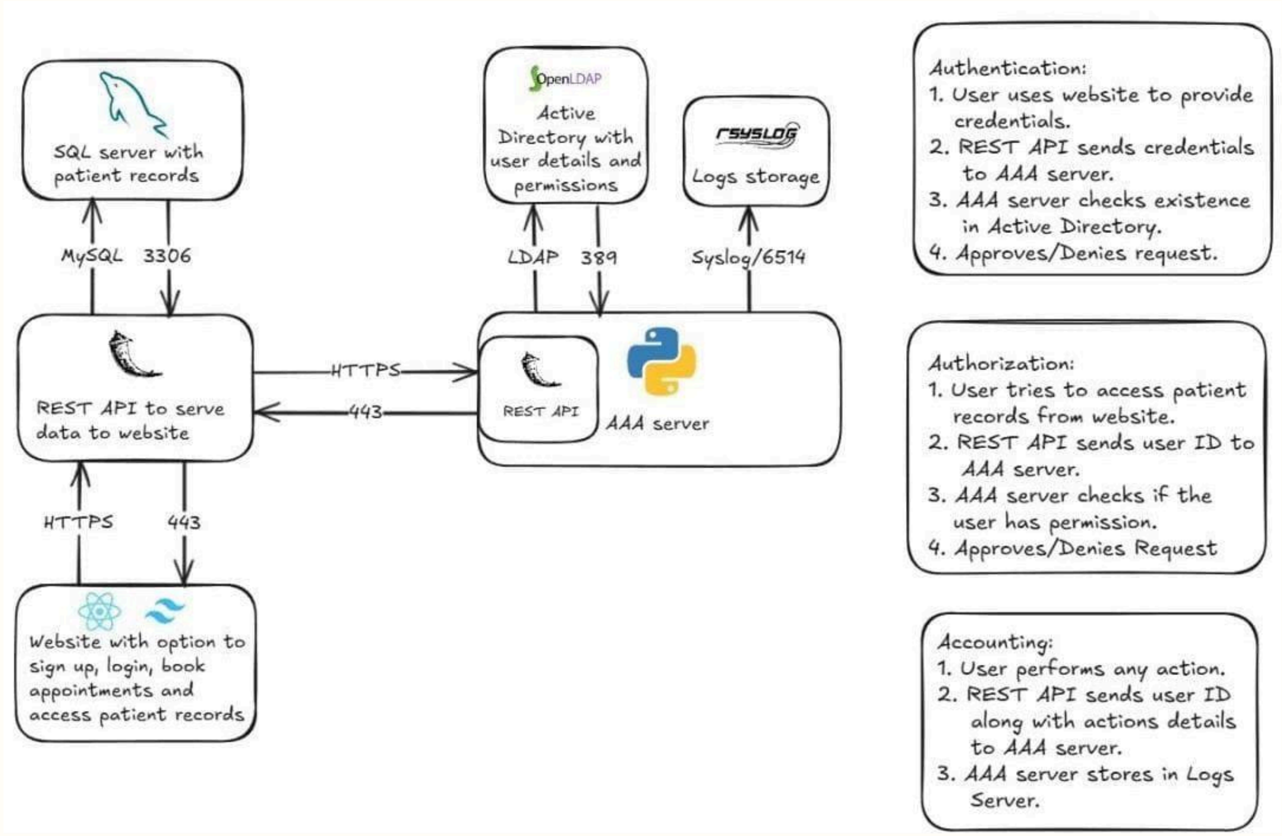
9.1 Data Flow Diagram

This diagram illustrates the security architecture for the psychiatric records app, showing how the Android app communicates securely (over HTTPS) with backend services in a protected virtual machine network. Users log in on the app using their password (checked via LDAP) and a one-time password (OTP) as a second authentication factor. The authentication service issues a secure token (JWT), allowing access to specific patient, history, and medication APIs which enforce strict, role-based access controls. All sensitive data is stored in an encrypted PostgreSQL database, while detailed audit logs are sent securely to a central logging system for monitoring. This setup ensures that patient records remain confidential, multi-factor authentication is enforced, and every access or activity is logged and protected across every layer of your system.

LINK: https://miro.com/app/board/uXjVJKrafUw=/?share_link_id=818987394906


TRUST BOUNDARY (FRONTEND/CLIENTS)
ANDROID (APK)
Login -> OTP -> Role based UI
JWT access + refresh
HTTPS 443 (Bearer JWT)
HTTPS 443 (login/password)
SECURE SERVICES NETWORK (VMs)
AAA Auth Service (Fast API)
🔒 Authentication Endpoints
/auth/login
/auth/verify
/auth/jwks.json
/auth/introspect
🛡 Authentication Mechanisms
Password via LDAP
MFA: OTP
Issues JWT (RS256)
Stores OTP hash + TTL
LDAPS 636 (service/user bind)
OpenLDAP (Identity + Groups)
System uses LDAPS (port 636) for read-only AAA access, Syslog over TLS (port 6514) for secure logging
Central Logs (rsyslog)
Syslog/TLS 6514 • JSON per host/day
JWKS / introspect
Resource API (FastAPI)
Endpoints /patients, /notes, and /meds are protected by a Policy Enforcement Point (PEP) that enforces role-based access control (RBAC), acts as a step-up gate, and emits audit events
Syslog TLS 6514
TLS 5432
APPLICATION DATABASE (PostgreSQL)
PATIENT • THERAPY_NOTES • MEDICATIONS • MFA_SESSION
At-rest: AES-256-GCM per-record DEK (wrapped by KMS/vault) • argon2id for local passwords.

Users access the website, where their credentials are sent securely to a Python-based AAA (authentication, authorization, accounting) server. This server checks usernames and permissions through an Active Directory (OpenLDAP), ensuring only approved individuals can log in and access records. Once authenticated, the AAA server verifies whether the user has permission to view specific patient data, before allowing the REST API to fetch that data from the SQL server and send it back to the website securely. Meanwhile, every user action; such as logins or record views, is recorded by the AAA server and stored in a log system for audit and compliance. All connections use encrypted channels, and the system enforces strict checks at every step to maintain privacy, proper access control, and accountability for psychiatric patient records.

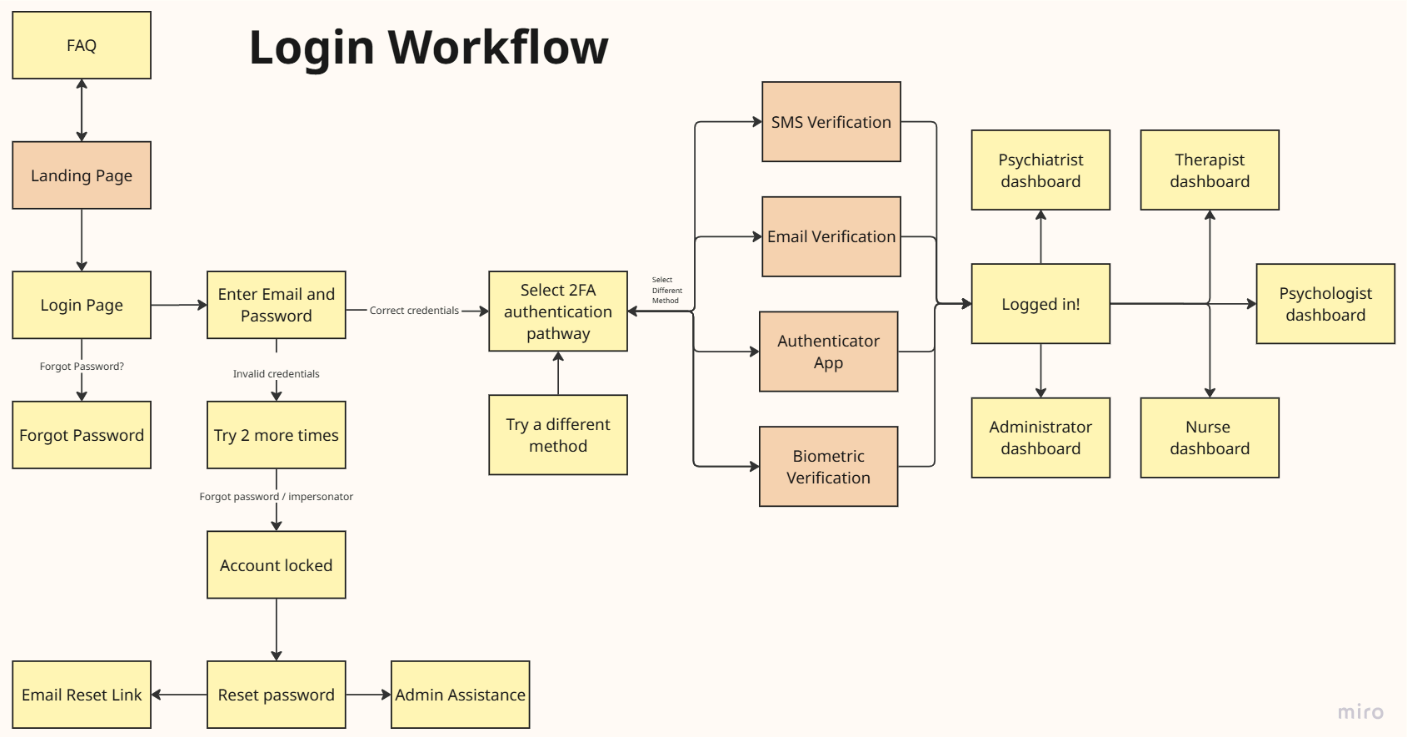

SQL server with patient records
MySQL
3306
OpenLDAP
Active Directory with user details and permissions
LDAP
389
rsyslog
Logs storage
Syslog/6514
REST API to serve data to website
HTTPS
443
REST API
AAA server
HTTPS
443
Website with option to sign up, login, book appointments and access patient records

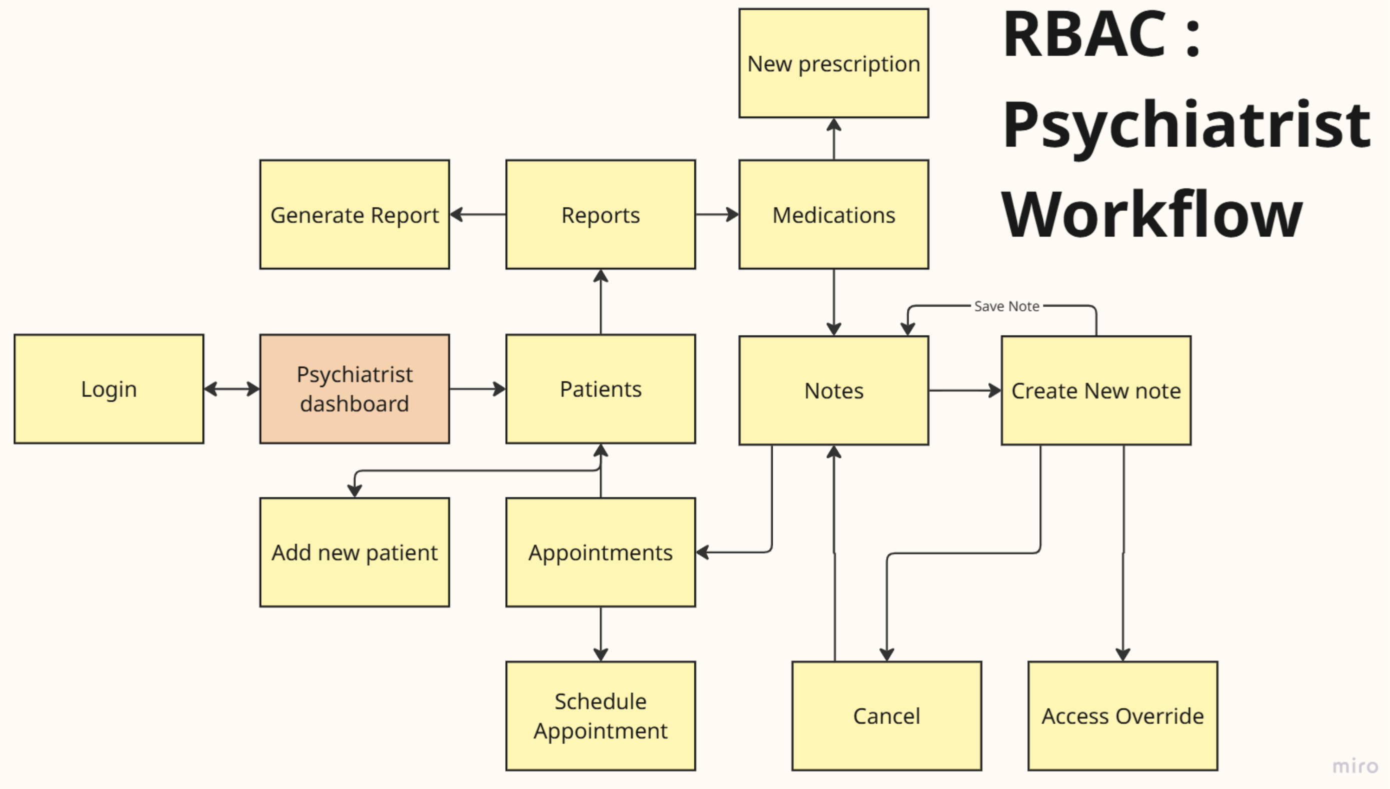
Authentication:
1. User uses website to provide credentials.
2. REST API sends credentials to AAA server.
3. AAA server checks existence in Active Directory.
4. Approves/Denies request.

Authorization:
1. User tries to access patient records from website.
2. REST API sends user ID to AAA server.
3. AAA server checks if the user has permission.
4. Approves/Denies Request

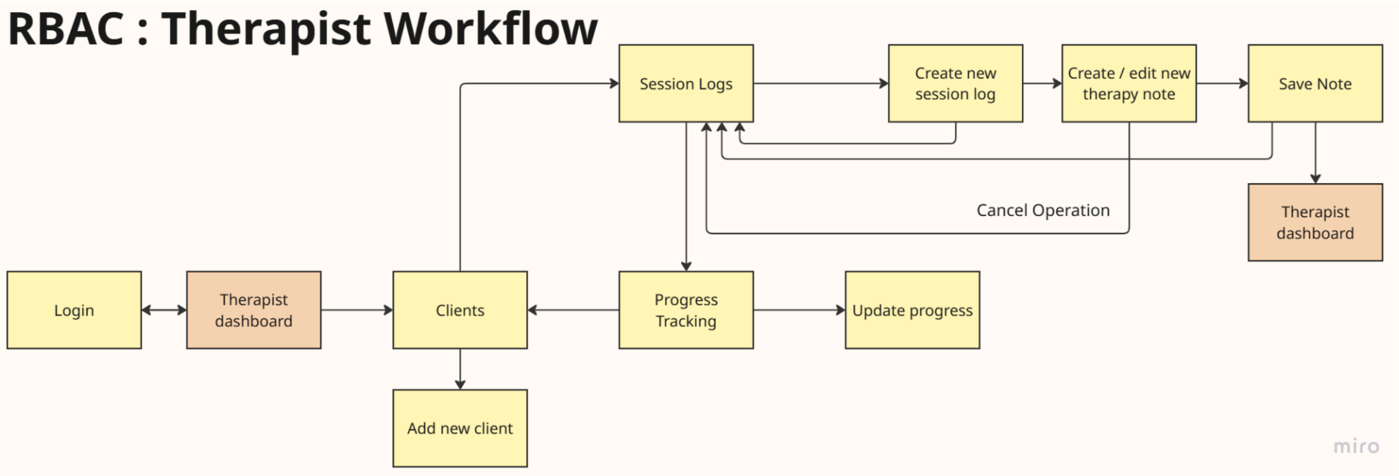
Accounting:
1. User performs any action.
2. REST API sends user ID along with actions details to AAA server.
3. AAA server stores in Logs Server.

9.2 RBAC Workflows and Login LINK

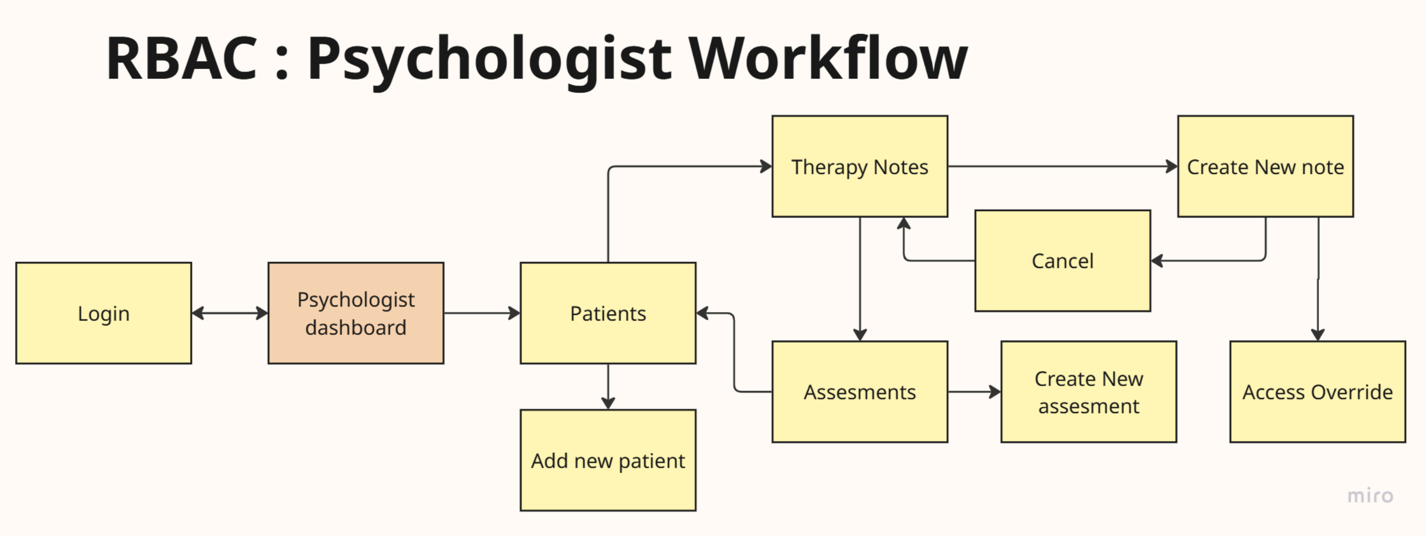




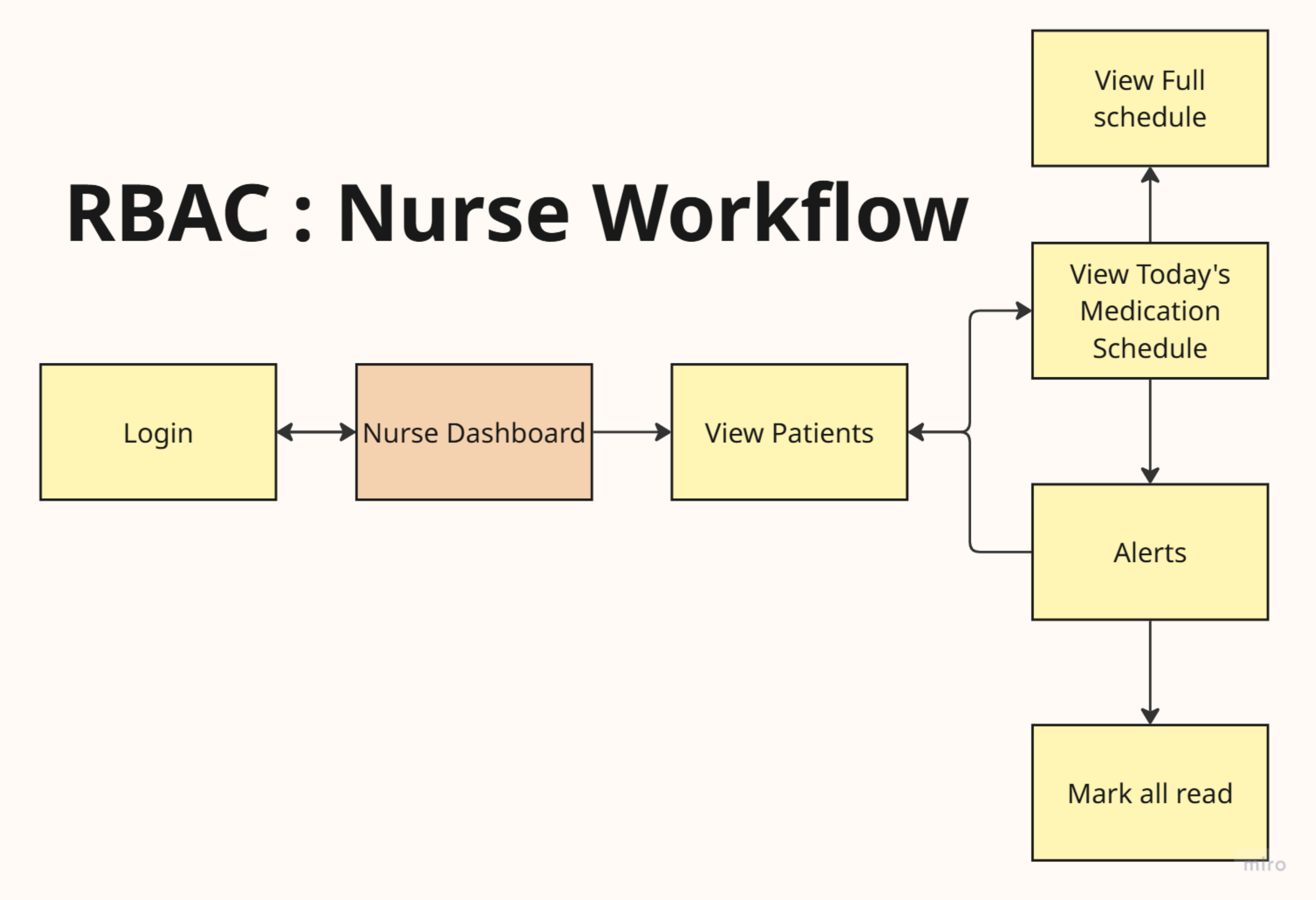
RBAC : Psychiatrist Workflow



RBAC : Therapist Workflow



RBAC : Psychologist Workflow



RBAC : Nurse Workflow

Login

Nurse Dashboard

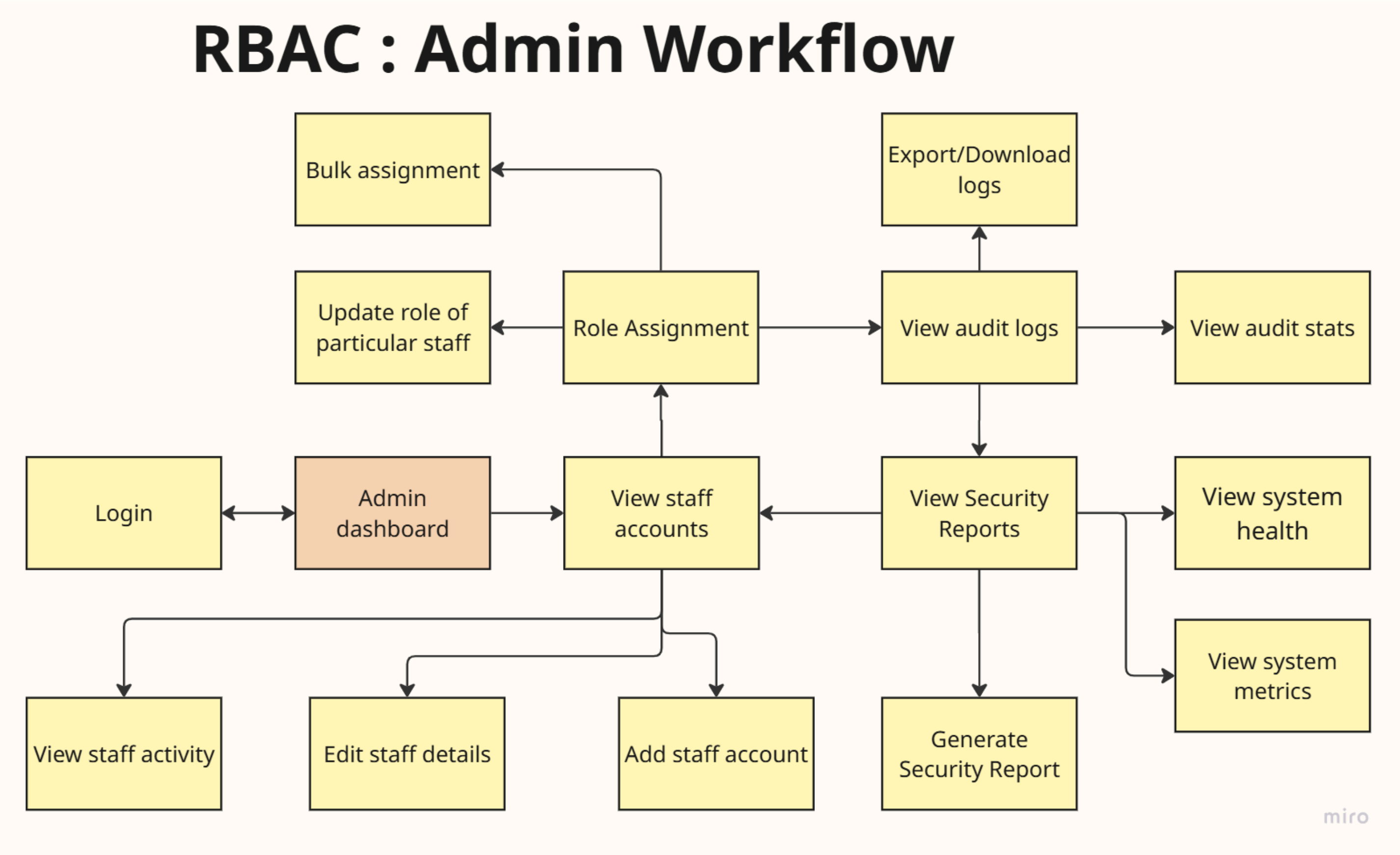
View Patients

View Today's Medication Schedule

View Full schedule

Alerts

Mark all read



RBAC : Admin Workflow

Login

Admin dashboard

View staff accounts

Role Assignment

Bulk assignment

Update role of particular staff

View audit logs

Export/Download logs

View audit stats

View Security Reports

View system health

View system metrics

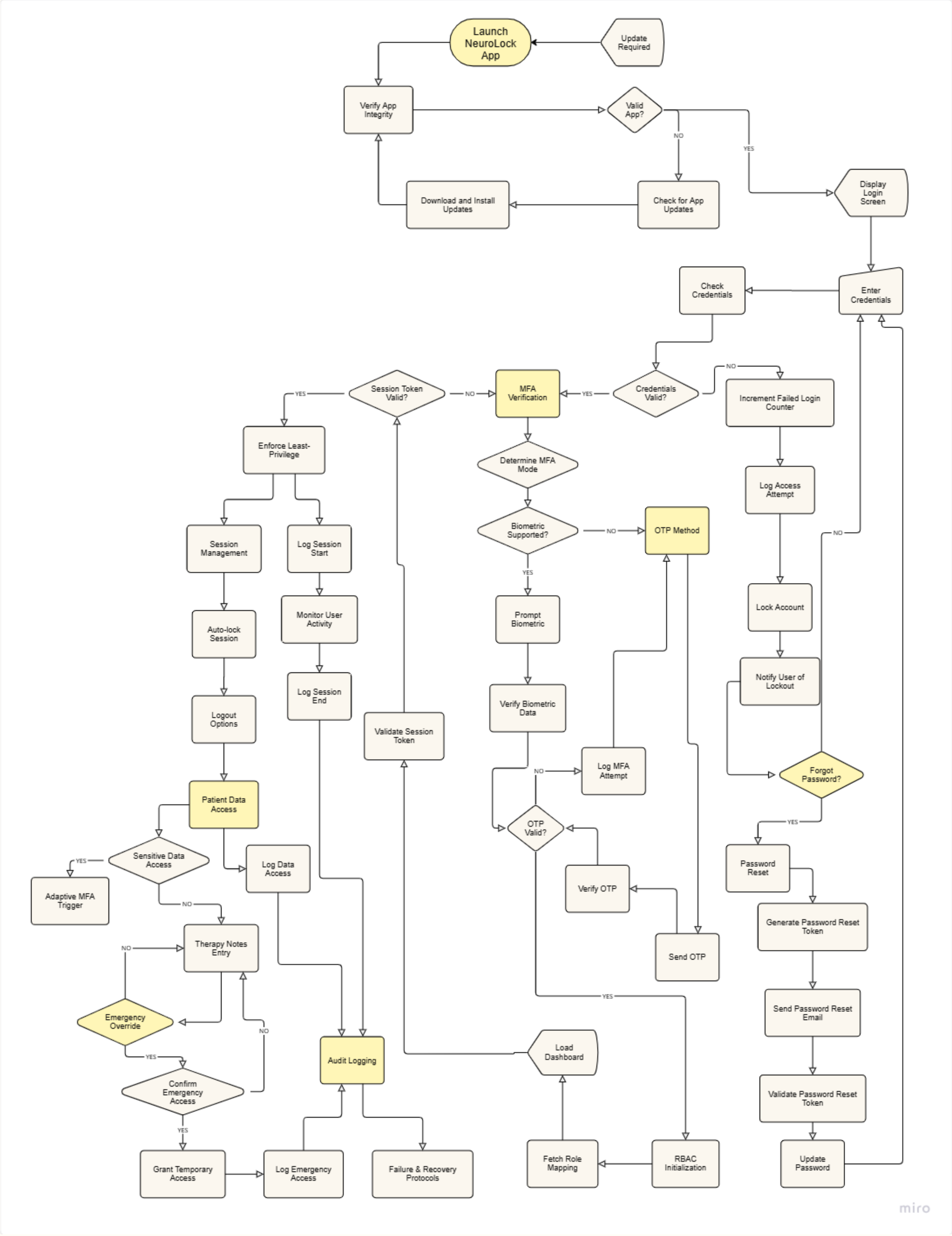
View staff activity

Edit staff details

Add staff account

Generate Security Report

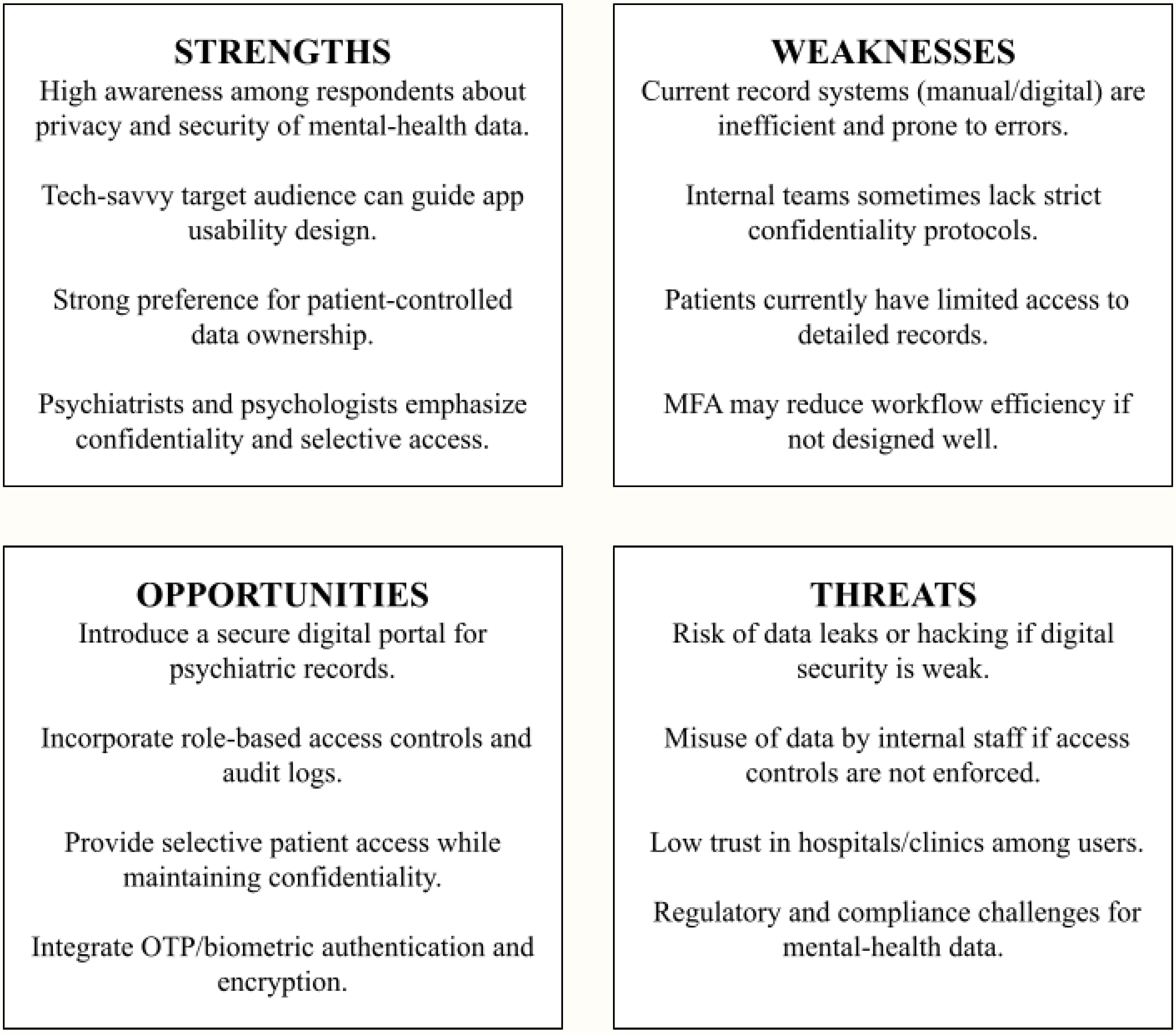
9.3 Security focused Workflow



9.4 System Architecture Document (additional): LINK

10. Analysing all the data till now

10.1 SWOT Analysis



STRENGTHS

High awareness among respondents about privacy and security of mental-health data.

Tech-savvy target audience can guide app usability design.

Strong preference for patient-controlled data ownership.

Psychiatrists and psychologists emphasize confidentiality and selective access.

WEAKNESSES

Current record systems (manual/digital) are inefficient and prone to errors.

Internal teams sometimes lack strict confidentiality protocols.

Patients currently have limited access to detailed records.

MFA may reduce workflow efficiency if not designed well.

OPPORTUNITIES

Introduce a secure digital portal for psychiatric records.

Incorporate role-based access controls and audit logs.

Provide selective patient access while maintaining confidentiality.

Integrate OTP/biometric authentication and encryption.

THREATS

Risk of data leaks or hacking if digital security is weak.

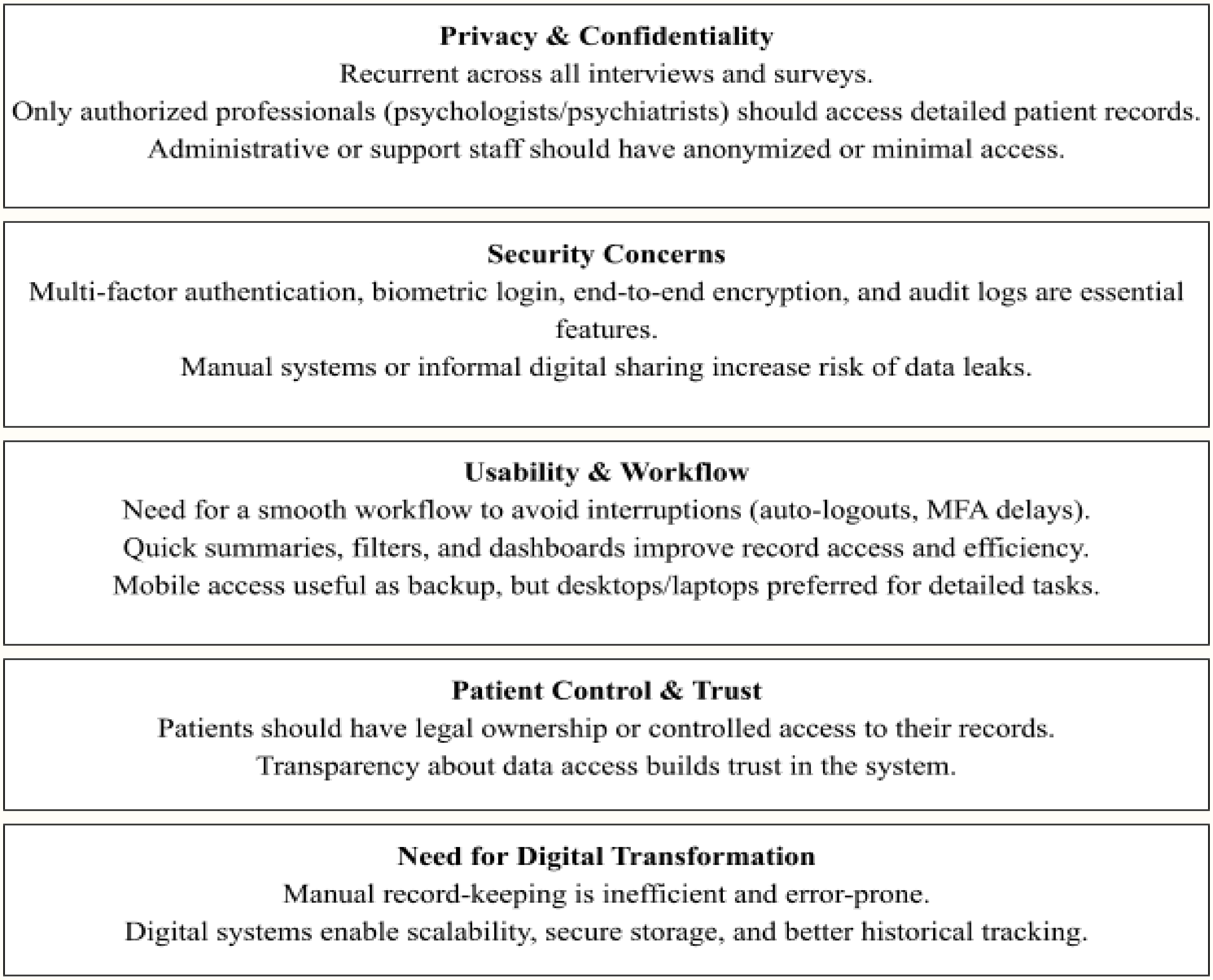
Misuse of data by internal staff if access controls are not enforced.

Low trust in hospitals/clinics among users.

Regulatory and compliance challenges for mental-health data.

10.2 Thematic Analysis

The diagram below illustrates the themes that arised from previously conducted research.



Privacy & Confidentiality

Recurrent across all interviews and surveys.

Only authorized professionals (psychologists/psychiatrists) should access detailed patient records.

Administrative or support staff should have anonymized or minimal access.

Security Concerns

Multi-factor authentication, biometric login, end-to-end encryption, and audit logs are essential features.

Manual systems or informal digital sharing increase risk of data leaks.

Usability & Workflow

Need for a smooth workflow to avoid interruptions (auto-logouts, MFA delays).

Quick summaries, filters, and dashboards improve record access and efficiency.

Mobile access useful as backup, but desktops/laptops preferred for detailed tasks.

Patient Control & Trust

Patients should have legal ownership or controlled access to their records.

Transparency about data access builds trust in the system.

Need for Digital Transformation

Manual record-keeping is inefficient and error-prone.

Digital systems enable scalability, secure storage, and better historical tracking.

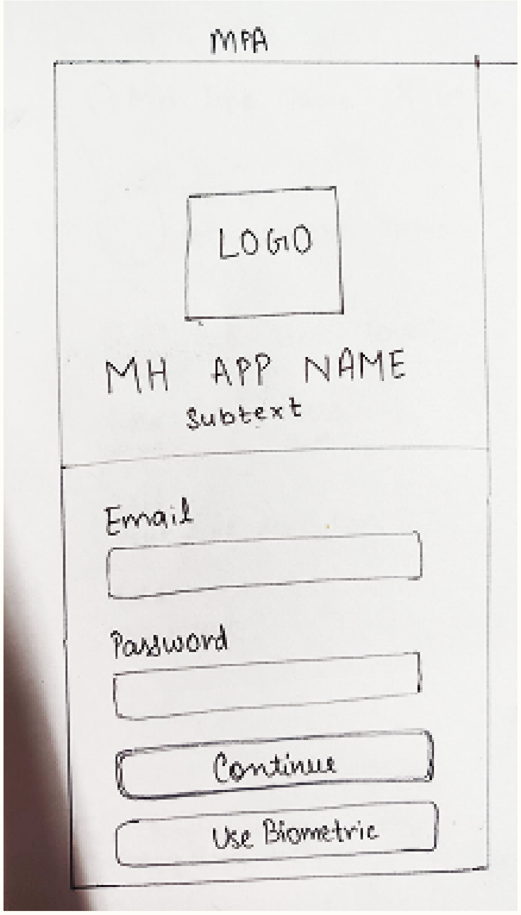
11. Paper Lo-fi Prototyping

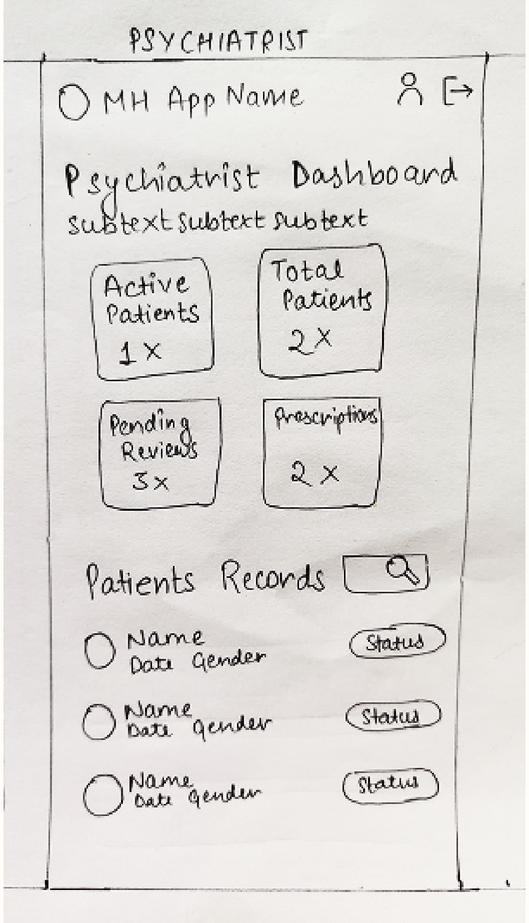
11.1 Overview

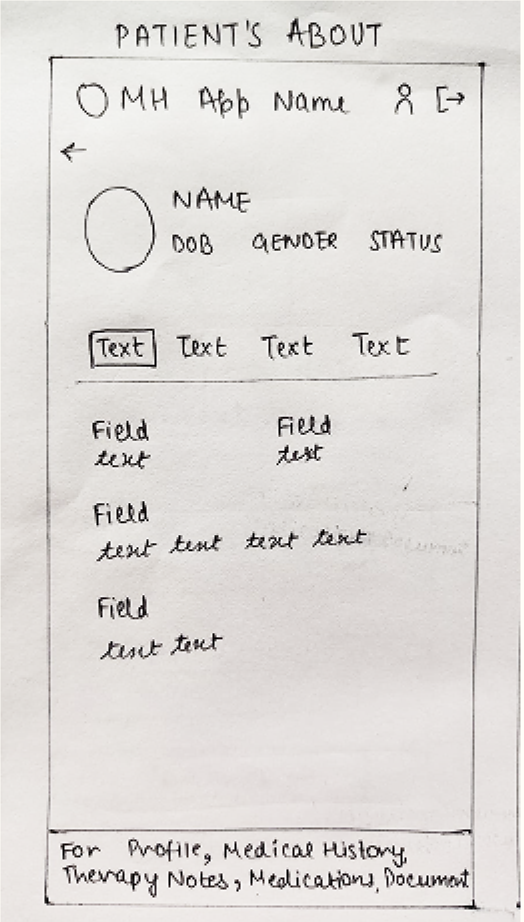
This prototype builds from the insights received earlier. There is a Login page asking for email and password, and biometrics. OTP verification page. Role-based dashboards for Psychiatrists, Therapists, and Nurses. An About Page for the patient. And also Admin dashboard along with Audit Logs.

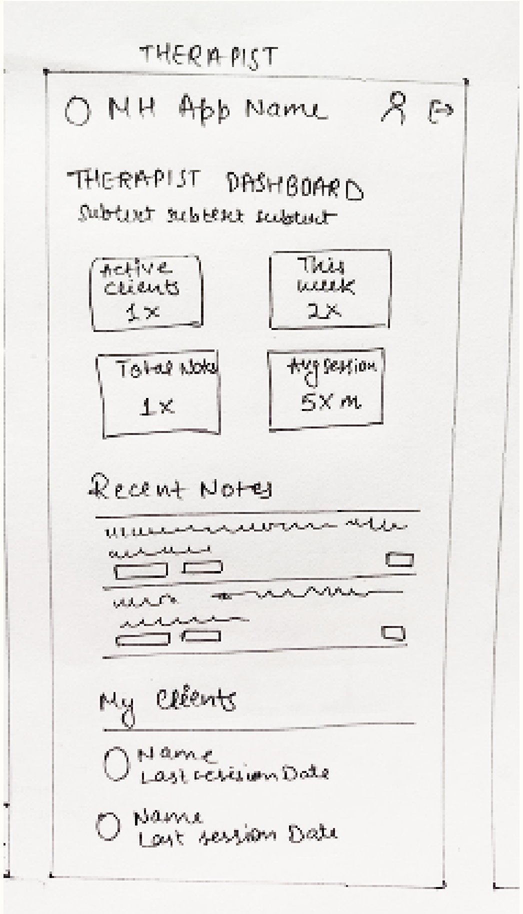
11.2 Frames

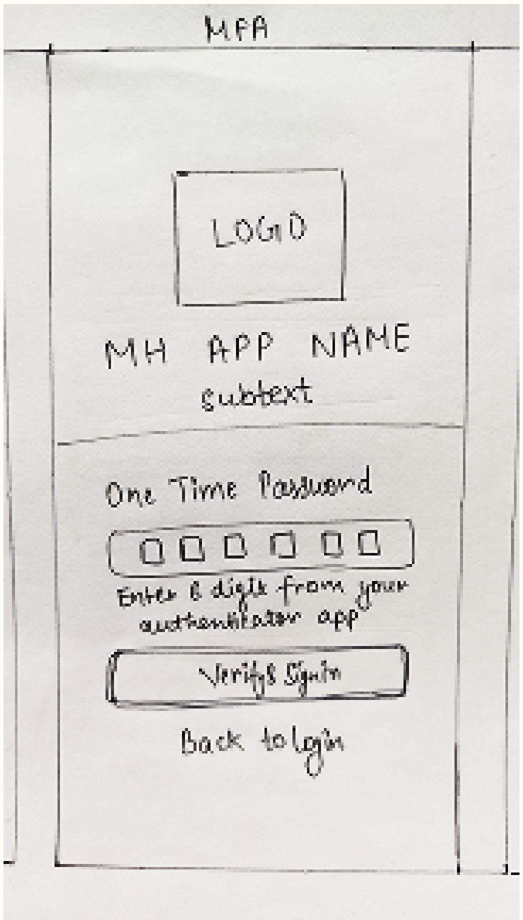
Given below.

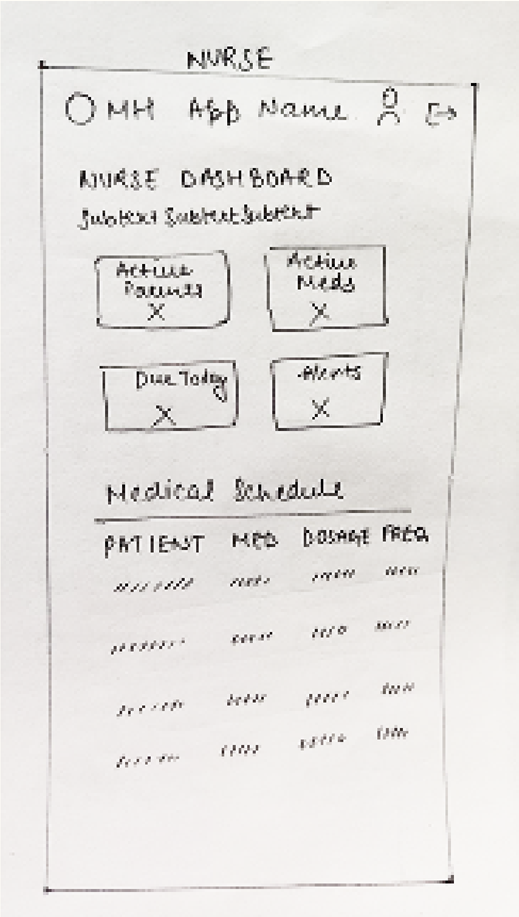

MFA
LOGO
MH APP NAME
Subtext
Email
Password
Continue
Use Biometric

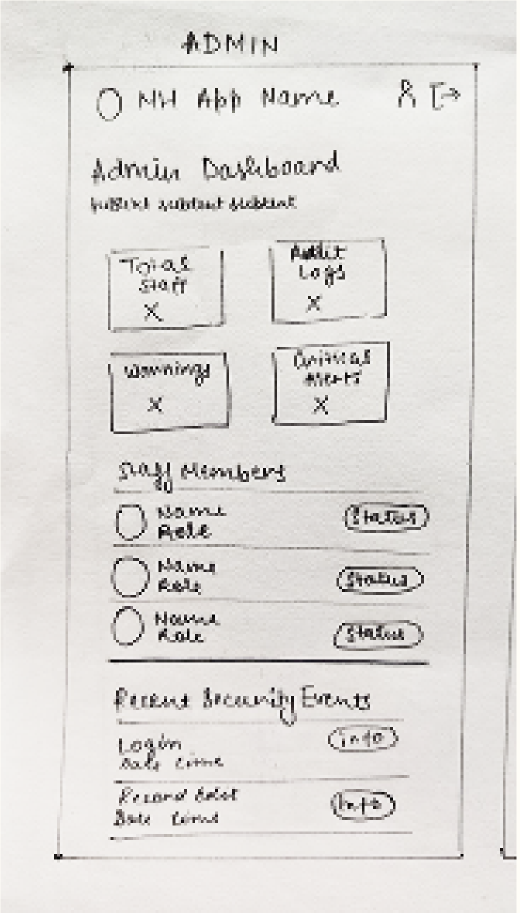

PSYCHIATRIST
MH App Name
Psychiatrist Dashboard
subtext subtext subtext
Active Patients 1X
Total Patients 2X
Pending Reviews 3X
Prescriptions 2X
Patients Records
Name Date Gender Status
Name Date Gender Status
Name Date Gender Status

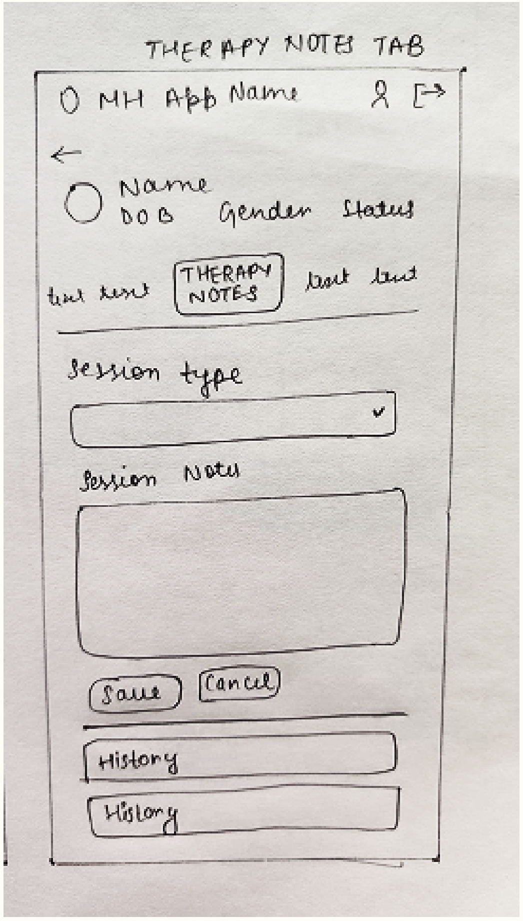

PATIENT'S ABOUT
MH App Name
NAME
DOB GENDER STATUS
Text Text Text Text
Field text
Field text
Field
text text text text
Field
text text
For Profile, Medical History, Therapy Notes, Medications, Document

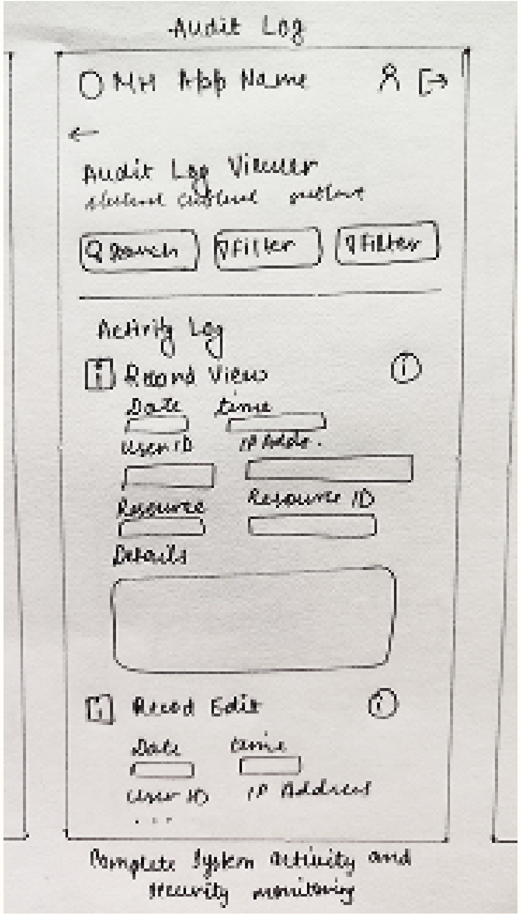

THERAPIST
MH App Name
THERAPIST DASHBOARD
Subtext subtext subtext
Active Clients 1X
This week 2X
Total Notes 1X
Avg session 5X m
Recent Notes
My Clients
Name Last session Date
Name Last session Date


MFA
LOGO
MH APP NAME
subtext
One Time Password
Enter 6 digits from your authenticator app
Verify Signin
Back to login


NURSE
MH App Name
NURSE DASHBOARD
subtext subtext subtext
Active Patients
X
Active Meds
X
Due Today
X
Alerts
X
Medical Schedule
PATIENT
MED
DOSAGE
FREQ


ADMIN
MH App Name
Admin Dashboard
subtext subtext subtext
Total Staff
X
Audit Logs
X
Warnings
X
Critical Alerts
X
Staff Members
Name
Role
Status
Name
Role
Status
Name
Role
Status
Recent Security Events
Login
Date time
Info
Record Edit
Date time
Info


THERAPY NOTES TAB
MH App Name
Name
DOB
Gender
Status
text text
THERAPY NOTES
text
text
Session type
Session Notes
Save
Cancel
History
History



Complete System activity and security monitoring

12. Post-Lofi Research

12.1 Overview

Objective: To understand user perceptions, concerns, and preferences about mental-health apps, privacy, and therapy-seeking behavior after creating a low-fidelity prototype. Purpose was to identify user frustrations, satisfaction levels with our current lo-fi to improve it in next iteration. Understand if our lo-fi security and privacy aspects fulfill their needs.

Target Group:
57 respondents
UsS Course students, IIIT Delhi
Age: 18–24 years
Field: Computer Science
Education Level: Undergraduate

Research Type:
Offline interviews with a supporting survey, Focus Group Discussions with maximum 5 people
Combination of multiple-choice, Likert scale (1–5), and open-ended questions

Focused on technology comfort, therapy attitudes, privacy concerns, trust in professionals, and app security features

Methodology:

1. Consent was taken with a form and for recording audio
2. Explained the Lo-fi, the design theme, and working
3. Asked questions about each page
4. Interviewees answered 47 structured questions
5. Data collected in Excel-ready format
6. Responses were anonymized and treated confidentially

12.2 Raw Findings

General Perception and Confidence in the Lo-Fi Prototype:
The overall reaction to the lo-fi prototype was highly positive, with responses like comprehensive and clear. The prototype was deemed to have "*covered everything in detail*". Frequently described as "*clean and understandable*" and "*really handy*".

Login System:
The interaction with the login page got praise for its clarity and robust security measures. It was consistently rated highly for clarity, receiving ratings of five out of five. 5/5
The design of the login page made users feel that their account and the data stored within would be secure. The addition of a Multi-Factor Authentication (MFA) step, with SMS and email authentication, authenticator apps (such as Google Authenticator) and backup codes, was considered very effective in enhancing security, OTP being rated four or five out of five.
Biometric login (fingerprint, Face ID) was highlighted as a preferred option because it is "*time effective*" and considered a "*master password that cannot be hacked easily*".
The system should include security mechanisms such as locking the account after a maximum of three invalid attempts, and providing clear recovery steps (using backup codes).

Role-Based Access Control (RBAC) and Dashboard Layouts:

1. **Psychiatrist Dashboard**: Users were highly confident (rated 4-5 out of 5) that only psychiatrists, and not other staff, could view these highly sensitive medical and therapy details.
2. **Psychologist Dashboard**: The system was specifically designed so that Psychologists can see therapy notes, assessments (tests), and the patient list, but "cannot see medical (drugs/prescriptions) information".
3. **Therapist Dashboard**: Therapist layout that contains session logs, notes, and progress to recovery was observed to be effective. The session notes process, with date, time, type, clinical assessment, and treatment, was intended to be "simple to fill as possible" as it was practical to complete and to save automatically
4. **Nurse Dashboard**: The layout was designed to strictly limit access. Users were comfortable with nurses viewing and managing only the medication schedule, dosage, and frequency. The layout was explicitly clear that nurses "do not have access to your full medical and therapy history".
5. **Administrator Dashboard**: The Admin manages staff (doctors, nurses) and tracks security events. Crucially, the prototype design confirmed that the Admin "cannot see the actual data". Instead, the Admin monitors audit logs and recent security events to track who accessed what data, ensuring system integrity rather than patient detail visibility. Users were highly comfortable with this level of monitoring.

Specific Usability and Feature Feedback:
Respondents offered specific suggestions to enhance the usability and privacy within the design:

1. **Practicing Anonymity**: A key suggestion for patient anonymity on dashboards was to use an "assigned ID or initials" instead of the client's full name when briefly displaying patient information, giving a "very little insight" while protecting the patient.
2. **History Feature**: The history function, which allows therapists to track previous session notes, was found to be "pretty clear". However, a recommendation was made to display notes "step by section" rather than all at once.
3. **Reporting Security Breaches**: A suggestion was made to include an option for the Admin to report a privacy breach.
4. **Reports Section**: The inclusion of a dedicated Reports section for psychiatrists was singled out as an important feature, especially since they deal with high-profile, high-risk cases.

Proposed Back-End Security Features:

1. The proposal to implement restrictions that disallow screen-shotting and copying of text within the entire application was highlighted as crucial for highly sensitive notes and was well received by the users as it made them feel "*more secure*".
2. The system's tracking of audit logs for "every single action" (accessing data, editing notes) allows the Admin to manage security events and determine "who accessed what data" if a security breach occurs.

12.3 Current Observed Limitations

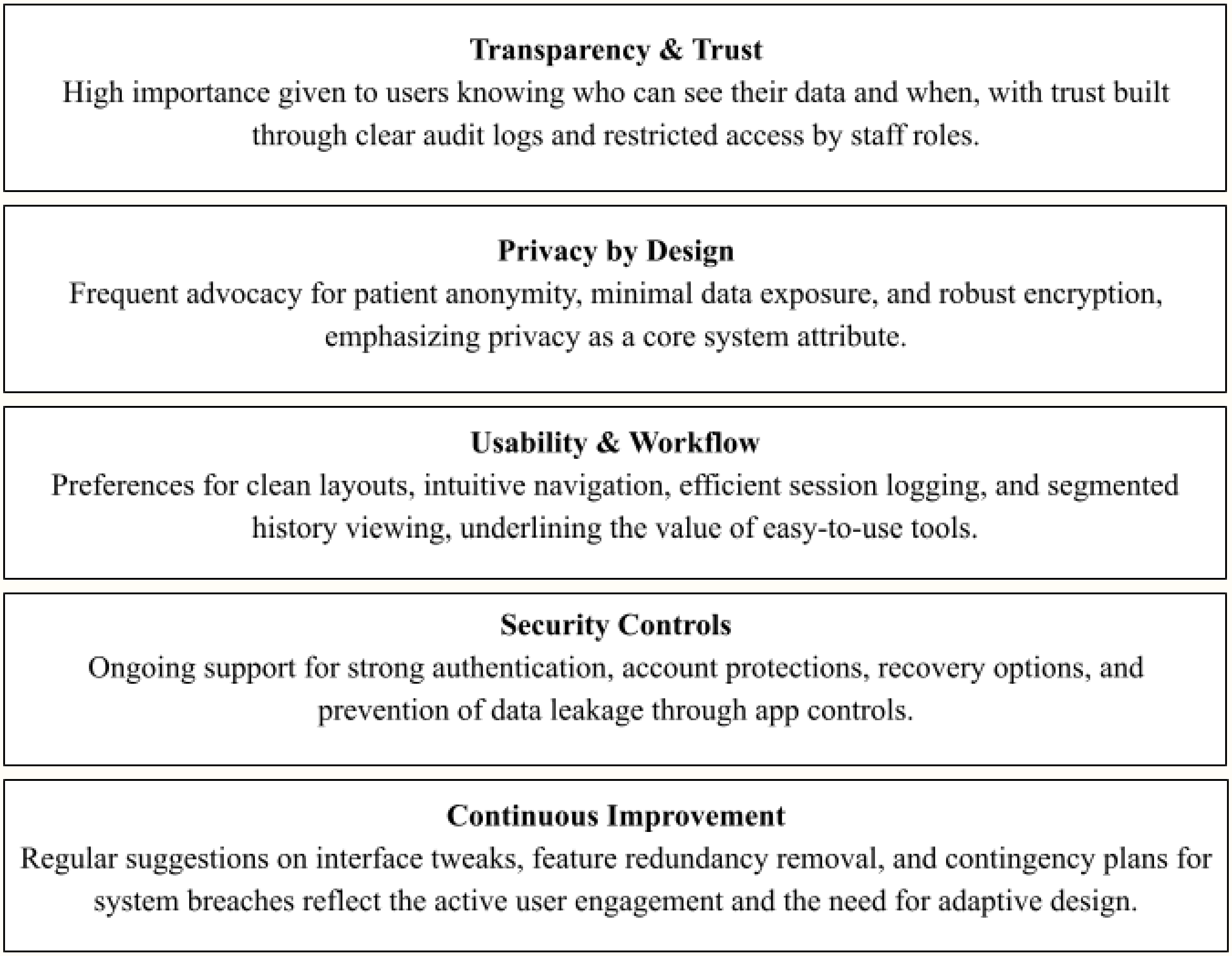
1. **Anonymity Practices**: Patient names appear in dashboards, exposing personal identity; replacing names with patient IDs or initials was frequently recommended to protect anonymity.
2. **History Feature Overload**: The history function displays all session notes at once, making it difficult for users to navigate; presenting notes section-wise or in a stage-wise manner could improve clarity and usability.
3. **Security for Laypersons**: While security mechanisms are robust for technical users, the system might not convey its security features clearly enough to non-technical users; efforts should be made to visually and verbally indicate protection status.
4. **Error Prevention**: Some users were concerned about what they are supposed to do if suppose their account is locked, or the therapist needs supervision or a new device needs to be registered, among other cases.
5. **Redundancy and UI Efficiency**: Elements like the “Back to Login” button were sometimes perceived as unnecessary and could be removed for a cleaner interface.

12.4 Proposed Improvements

1. **Authentication Enhancements:** Add passkeys, enable direct logins via options like phone number or Google, and ensure options for forgotten passwords and backup authentication codes.

2. **Reporting and Response:** Implement an option for users and administrators to report suspicious activity or privacy breaches, and create a protocol for isolating or shutting down systems in the event of a breach.
3. **Flexible Data Views:** Allow two-step or stage-wise access to patient records, particularly sensitive sections; add filter options to dashboards for easier data navigation and management.
4. **Screen Capture Prevention:** Complete the proposed restriction against screenshots and text copying, especially for highly sensitive content, to minimize risk of information leakage.
5. **User Experience Improvements:** Refine history features for segmented note viewing, optimize design for better visual appeal, provide clear instructions for all user actions, and ensure that the system caters to all patient needs, including beyond medication schedules (e.g., sessions and assessments).

12.5 Thematic Analysis



Transparency & Trust

High importance given to users knowing who can see their data and when, with trust built through clear audit logs and restricted access by staff roles.

Privacy by Design

Frequent advocacy for patient anonymity, minimal data exposure, and robust encryption, emphasizing privacy as a core system attribute.

Usability & Workflow

Preferences for clean layouts, intuitive navigation, efficient session logging, and segmented history viewing, underlining the value of easy-to-use tools.

Security Controls

Ongoing support for strong authentication, account protections, recovery options, and prevention of data leakage through app controls.

Continuous Improvement

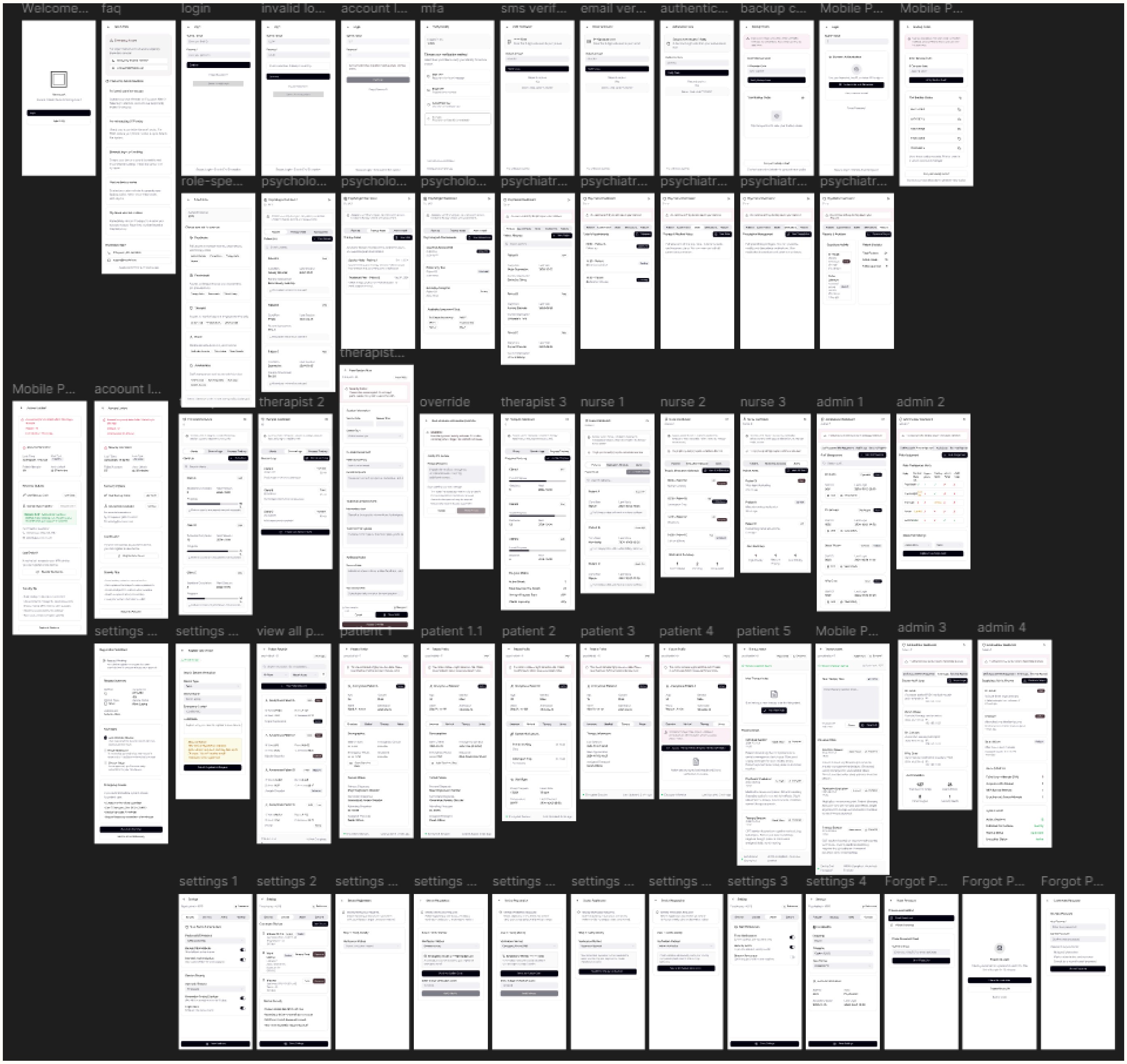
Regular suggestions on interface tweaks, feature redundancy removal, and contingency plans for system breaches reflect the active user engagement and the need for adaptive design.

13. Digital Mid-fi Prototype on Figma

13.1 Overview

This prototype builds from the insights received earlier. There are total 57 comprehensive wireframes that include Login, MFA, forgot password, account lock, registering for new device, RBAC dashboards, therapy notes, audit logs, access override, settings and more.

https://www.figma.com/design/RbQUzFH7bFXPTqWcNpO71W/neurolock?node-id=0-1&t=iU5thJC7ImLmzqfi-1



13.2 Key Features

Core Security & Authentication

1. **Multi-Factor Authentication System**: Complete MFA implementation with SMS, email, authenticator app, and biometric verification options, plus intelligent method selection based on login type
2. **Biometric Login Integration**: Device-native fingerprint/face ID authentication with fallback options and smart MFA routing
3. **Account Protection & Recovery**: Automatic lockout after failed attempts, backup codes, device registration flow, and emergency contact systems
4. **Role-Based Access Control**: Five distinct staff roles (Psychiatrist, Psychologist, Therapist, Nurse, Admin) with granular permission systems

Patient Data Management

1. **Secure Patient Records System**: Comprehensive patient profiles with medical history, prescriptions, therapy notes, and assessment data tailored to staff permissions
2. **Adaptive Re-Authentication**: Dynamic security prompts for accessing sensitive therapy notes with HIPAA compliance messaging
3. **Therapy Notes Editor**: Full-featured secure note editor with autosave, version control, encryption indicators, and collaborative editing features
4. **Advanced Search & Filtering**: Patient discovery with multiple filters (condition, priority, age, last visit)

Administrative & Monitoring

1. **Comprehensive Audit & Logging**: Real-time staff activity tracking, security event monitoring, and administrative review workflows with detailed timestamps
2. **Security Alert Management**: Proactive threat detection including suspicious login patterns, after-hours access, and emergency override tracking
3. **Override System**: Critical access protocols with full audit trails, supervisor notifications, and security review processes

Resilience & Recovery

1. **Offline Mode Capabilities**: Limited functionality with cached patient data, network reconnection detection, and mandatory re-authentication
2. **Device Management & Registration**: Multi-step device approval process with identity verification, administrator oversight, and trusted device management
3. **Error Recovery Flows**: Account unlock procedures, lost device registration, forgot password recovery, and emergency access protocols

User Experience & Settings

Comprehensive Settings & Personalization: Security preferences, MFA method selection, device trust management, notification controls, and multi-language localization support

13.3 Usability Feedback of Mid-Fi (Interviews)

Participants: 7 college students, IIIT Delhi
Each was briefed on the context of hospital operations and patient data sensitivity before testing.
Interviews lasted 10-15 minutes each.

Methodology

1. Log in using MFA
2. Navigate to every role's dashboard
3. Access a patient record and attempt to view therapy notes
4. Trigger adaptive re-authentication
5. Attempt an override
6. Logout and review audit log

Users described the NeuroLock prototype as secure, comprehensive, and highly organized. They said that it handled a wide range of real-world scenarios smoothly like login, MFA, and data entry. And also overrides and recovery flows. The interface was praised for being clear, consistent, and intuitive. They shared that security steps "*felt logical, not intrusive*." Participants highlighted that the system "*anticipated every situation*," calling its design "*professional and well-structured*." The biometric MFA, auto-lock privacy cues, and role-based dashboards were repeatedly cited as standout features. Overall, feedback was strongly positive, confirming that NeuroLock achieves usable security through thoughtful design.

13.4 Future Work - Phase II

The next phase of NeuroLock will focus on turning the designed prototype into a fully functional Android application. The backend implementation will include building secure authentication, multi-factor authentication (MFA), and role-based access control (RBAC) APIs, along with audit logging, data encryption, and error recovery mechanisms. A virtual machine (VM) will be used for backend hosting and storage. On the frontend, the Figma prototype will be converted into a working Android APK using Java/Kotlin, integrating biometric login, OTP verification, adaptive MFA prompts, and offline mode functionality. The system integration phase will ensure seamless communication between frontend and backend through secure token-based sessions and consistent data flow across MFA, dashboards, and audit logs. Finally, extensive usability and security testing will be conducted for all user roles and error cases, alongside cross-testing of at least eight other group projects with all vulnerabilities and usability issues documented for review.

RESEARCH EVIDENCE COMPILED (Consent forms, recordings etc)

Thank you.

-Team VirUsS