Summary of Findings: Privacy and Anonymization for Hospital Speech Recognition AI

submitted by: Nayana Jacob Alappattu

My analysis focused on privacy compliance, anonymization techniques, and operational safeguards essential for deploying an AI-powered speech recognition system in a hospital context, emphasizing GDPR compliance.

The General Data Protection Regulation (GDPR) recognises data concerning health as a special category of data and defines health data for data protection purposes and necessitating additional safeguards.[1] Potential speaker re-identification, unwanted access, and health state inference based on speech attributes are all privacy risks.
Here, three anonymization methods are used: pitch shifting (+5 semitones), time stretching(1.5x), and McAdams coefficient method(α=0.8). The results showed a privacy-utility tradeoff: McAdams gained the highest transcription accuracy with minimal anonymization, pitch shifting enhanced privacy but reduced accuracy, and time-stretch decreased intelligibility and privacy evaluation since it fails to anonymize properly. Limitations exist, as no strategy ensures irreversible anonymization; all methods may leave residual speaker-specific information vulnerable to advanced attacks. Anonymization has an impact on both usability (recognition accuracy) and user acceptance. Continuous validation with re-identification testing and expert review is recommended.

Open challenges and recommendations:

Balancing anonymization strength with transcription accuracy remains difficult, so adopting the strongest anonymization methods available with ongoing performance is recommended. The challenges of managing hospital speech recognition data under GDPR include ensuring that data processing is lawful, fair, and transparent despite complex clinical environments and patient concerns; restricting data use to specific, explicit purposes while accommodating legitimate secondary uses like research; collecting only essential data needed for the healthcare purpose; maintaining data accuracy amidst dynamic medical workflows; limiting data storage duration without compromising archiving and research needs; safeguarding data integrity and confidentiality to prevent breaches or corruption; and demonstrating accountability through documentation and proof of compliance. Corresponding **GDPR** principles address these by mandating transparent and lawful processing aligned with EU laws, purpose limitation allowing research reuse under strict conditions, data minimization to limit collection to relevant information, accuracy requirements with correction obligations, storage limitation with exceptions for scientific uses, security measures to uphold data integrity and confidentiality, and accountability that places the burden of proof on data controllers to show compliance. Together, these principles form a framework of safeguards and recommendations that help hospitals overcome practical data protection challenges when implementing speech recognition technologies.[2]

[1] https://www.edps.europa.eu/data-protection/our-work/subjects/health_en

[2] https://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf