TABLE 8: Full Codebook

Current Practice of Identity Verification	Perception of PHC	Design Preference of PHC
Current practices about verification-2FA	Pre understanding: related to biological feature	Design preference: adding valid time constraints
Current practices about financial verification: gov id (SSN/driver's licence/photo id)	Pre understanding: daily life verification	Design preference: third-party commitments
Current practices about financial verification-face	Pre understanding: another type of person identification	Design preference: encrypted credentials
Current practices about financial verification-fingerprint	Pre understanding: identity verification with uniqueness-personality, appearance, behavioral-patterns	Design preference: checking orgnizations
Current practices about social media-no identification	Pre understanding: knowledge-based authentication	Design preference: transparency-what information is going to be shared
Current practices about in-person verification	Post understanding: everything stored in database	Design preference: segregating database-preventing access to irrelevant or sensitive information
Biometric depends on devices	Post understanding: Similarity to SSL technology-encryption and hashing	Design preference: platforms should be accessible and available
Biometrics is easier no need to remember credentials	Post understanding: Third-party certificate verification	Design preference: government involvement in PHC
External factors (appearance, light) influence face recognition	Post understanding: verifying that someone is a human being not AI	Design preferences: robust system with algorithm
Perception about biometric: face is faster than fingerprint	Benefits: verify uniquness / unique indvidual	Design preferences: education training to prevent social engineering
Perception about biometric: it will change after certain period time	Benefits: reduced exposure of personal information	Design preference: 2FA when interacting with service providers
Perception about biometric: can't be stolen as locally stored in device	Benefits: not needing multiple type of credential for different services	Design preference: platforms should be accessible and available
Verification problem with credential's validity period	Benefits: less repeated verification	Design preference: government involvement in PHC
Security concern about biometrics (face, iris, fingerprint)	Benefits: less risk of data linkage, data getting stolen	Design preferences: robust system with algorithm
Security concern about gov id	Benefits: less online identity issues-misinformation/malicious accounts	Design preferences: education training to prevent social engineering
Mental model: optimism towards technology	Benefits: less uploading documents	Design preference: 2FA when interacting with service providers
Lack of transparency/No idea how collected data will be used and shared	Benefits: easier and quicker than the usual verification	Design preference: mimicking blockchain structure
Confused understanding of authentication as verification	Benefits: more trusted 3rd party involvement	Design preference: ensuring database security, a 3rd party doing multi factor authentication
Regional Difference in verification Method: Social Media	Benefits: reduced risk of data linkage	Architecture preference: centralized for simplicity
Across border: Limitation in access/interoperability in verification method	Benefits: tracability decrease the chance of fake accounts	Architecture preference: middle - decentralized but oversight by gov
Current practices about verification - facial recognition matching photo id	Concerns: PHC/credentials getting stolen (due to hacking)	Architecture preference: decentralized improve security of centrailized data storage
Current practices about healthcare services: SSN/insurance information	Concerns: credential's validity period	Architecture preference: decentralized-users can choose preferred issuers
Perception about biometric: biometrc features can't be changed	Concerns: untrustworthy PHC issuer	Architecture preference: decentralized and sector-based
	Concerns: centralized data storage	Architecture preference: clear regulation/policy for decentralized
	Concerns: Issuers can be hacked	
	Concerns: PHC can be de-anonymized	
	Concerns: information will be stored centrally, this may lead to power can be abused later	
	Concerns: uncertain regulations	
	Concerns: failed to detect criminal information	
	Concerns: malicious attacker create fake PHC	
	Concerns: data linkage of credential and information stored in service providers	
	Credential: resistance to phisycal ID carrying	
	Credential: biometrics more secure than gov id	
	Credential: phone number as additional credential for security	
	Credential: SSN is enough for gov scenario	
	Credential: contextual preferences depends on service providers	
	Credential: accountability for biometric data collection	
	Stakeholders: comparison trustworthiness of PHC issuers and service providers	
	Stakeholders: trust government where they has already data access to all information	
	Stakeholders: trust with financial institution (secure/robust)	
	Stakeholders: distrust with social media companies	
	Stakeholders: distrust with LLM companies	
	Stakeholders: trust with healthcare	
	Stakeholders: trust with social media system	
	Mental model: perception face vs fingeprint vs iris scan	
	Mental model: how evaluate the trustworthiness of stakeholders	
	Mental model: perception biometric vs gov ID	
	Mental model: security perception Online vs. Direct video call for verification	
	Mental model: security perception Online vs. Direct Data Submission for verification	
	Transparency on data protection/security measures/regulations	
	Unnecessary PHC use in social media - reporting accounts is enough for fake accounts	