TABLE 9: 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	Credential preference: biometrics (work standalone without other credentials/easiness/secure)
Current practices about financial verification: gov id (SSN/driver's licence/photo id)	Pre understanding: daily life verification	Credential preference: email can be hacked easily, but won't reveal personal information
Current practices about financial verification: face	Pre understanding: another type of person identification	Credential preference: depends on who is issuing PHC
Current practices about financial verification: fingerprint	Pre understanding: identity verification with uniqueness-personality, appearance, behavioral-patterns	Credential preference: driver's license-it's common and people carry it almost always
Current practices about government verification: gov id	Post understanding: everything stored in database	Credential preference: government ID
Current practices about social media: no identification	Post understanding: Similarity to SSL technology-encryption and hashing	Credential preference: biometric as secondary option when forget id
Current practices about in-person verification	Post understanding: Third-party certificate verification	Stakeholder preference: trust with government
Biometric depends on devices	Benefits: reduced exposure of personal information	Stakeholder preference: government has already access to credential data
Biometrics is easier no need to remember credentials	Benefits: not needing multiple type of credential for different services	Stakeholders: trust financial institute where they have already data access to all information
Appearance factors influence face recognition	Benefits: less repeated verification	Stakeholders: distrust with third parties
External factors influence face recognition	Benefits: improved privacy	Stakeholders: financial institution is more secure
Perception about biometric: face is faster than fingerprint	Benefits: improved security	Design preference: adding valid time constraints
Perception about biometric: it will change after certain period time	Benefits: less risk of data linkage	Design preference: third-party commitments
Perception about biometric: can't be stolen as locally stored in device	Benefits: less online identity issues-misinformation/malicious accounts	Design preference: encrypted credentials
Verification problem with phone number	Benefits: less uploading documents	Design preference: checking organizations
Verification problem with credential's validity period	Benefits: less risk of data getting stolen	Design preference: transparency-what information is going to be shared
Security concern about face verification	Benefits: easier and quicker than the usual verification	Design preference: segregating database-preventing access to irrelevant or sensitive information
Security concern about iris verification	Benefits: more trusted 3rd party involvement	Architecture preference: decentralized improve security of centralized data storage
Security concern about fingerprint verification	Benefits: reduced risk of data linkage	Architecture preference: decentralized mitigates privacy concerns
Lack of transparency/No idea how collected data will be used and shared	Benefits: tracability decrease the chance of fake accounts	Architecture preference: decentralized-users can choose preferred issuers
Confused understanding of authentication as verification	Concerns: PHC/credentials getting stolen (due to hacking)	Architecture preference: decentralized and sector-based
Regional Difference in verification Method: Social Media	Concerns: credential's validity period	Architecture preference: clear regulation/policy for decentralized
Across border: Limitation in access/interoperability in verification method	Concerns: untrustworthy PHC issuer	Concerns: diverse user preferences who trust as issuers
Current practices about other services: govt id	Concerns: centralized data storage	Concerns: single credential across all information
Current practices about third-party verification	Concerns: Issuers can be hacked	Stakeholder preference: under the supervision of the government
Current practices about verification: facial recognition matching photo id	Concerns: PHC can de-anonymized	Stakeholders preference: PHC issuer and service providers are separated entities
Current practices about healthcare services: SSN/insurance information	Concerns: information will be stored centrally, this may lead to power can be abused later	Design preference: platforms should be accessible and available
Perception about biometric: biometrc features can't be changed	Concerns: uncertain regulations	Design preference: government involvement in PHC
No concerns on current practices with trustworthy stakeholders	Concerns: failed to detect criminal information	Design preferences: robust system with algorithm
Security concern about gov id	Concerns: malicious attacker create fake PHC	Design preferences: education training to prevent social engineering
Mental model: optimism towards technology	Concerns: data linkage of credential and information stored in service providers	Design preference: 2FA when interacting with service providers
	Credential: resistance to physical ID carrying	Architecture preference: centralized with biometric and gov. ID
	Credential: biometrics more secure than gov id	Architecture preference: centralized for simplicity
	Credential: phone number as additional credential for security	Architecture preference: middle-decentralized but oversight by gov
	Stakeholders: comparison trustworthiness of PHC issuers and service providers	Stakeholder preference: Union
	Stakeholders: trust with government	Design preference: mimicking blockchain structure
	Stakeholders: trust with financial institution (secure/robust)	Design preference: ensuring database security, a 3rd party doing multi factor authentication
	Stakeholders: distrust with social media companies	
	Stakeholders: healthcare system is less secure	
	Stakeholders: distrust with LLM companies	
	Stakeholders: trust with healthcare	
	Stakeholders: trust with social media system	
	Stakeholders: trust government where they have already data access to all information	
	Unnecessary PHC use in LLM	
	Unnecessary PHC use in healthcare	
	Unnecessary PHC use in government	
	Unnecessary PHC use in background check-receptiveness to data sharing	
	Unnecessary PHC use in social media-simple verification enough	
	Mental model: security perception Online vs. Direct Data Submission for verification	
	Trust on PHC depends on who is issuing PHC	
	Confusion about the entity who access to credential	
	Mental model: perception face vs fingerprint 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	
	Motivational experience using PHC	
	Transparency on data protection/security measures/regulations	
	Post understanding: verifying that someone is a human being not AI	
	Benefits: verify someone as legitimate	
	Benefits: verify uniqueness / unique individual	
	Concerns: credentials shared to other parties	
	Credential: SSN is enough for gov scenario	
	Credential: contextual preferences depends on service providers	
	Stakeholders: trust with background check companies	
	Stakeholders: trust with LLM companies	
	Stakeholders: distrust with 3rd party organizations	
	Unnecessary PHC use in social media - reporting accounts is enough for fake accounts	
	Similarity between healthcare and financial contexts	
	Similarity between social media and LLM contexts	
	Perception of technical systems as black boxes	
	Misunderstanding: PHC's tracability decrease criminal activities	
	Misunderstanding: Companies can track a person's activities with PHC	
	Pre understanding: knowledge-based authentication	
	Credential: accountability for biometric data collection	