SafeData 2.0 - Executive Summary

Problem Statement

National Statistical Office (NSO) releases anonymized microdata for researchers and policymakers. However, removing direct identifiers is insufficient - modern linkage attacks using auxiliary datasets can re-identify individuals, risking privacy and violating principles of DPDP Act, 2023 (purpose limitation, data minimization).

Proposed Solution

SafeData Pipeline: a modular privacy framework that balances privacy and utility. Core approach uses Synthetic Data Generation (SDG) plus Statistical Disclosure Control (SDC), with an adaptive SafeData 2.0 upgrade that integrates Differential Privacy in training, targeted SDC, attack simulation, and automated privacy-utility optimization.

Core Concepts

1. Synthetic Data Generation (SDG): create artificial records preserving statistical properties but containing no real persons. 2. Statistical Disclosure Control (SDC): targeted generalization/noise/suppression to remove risky, rare patterns. 3. Differential Privacy (DP): add formal, measurable privacy guarantees (epsilon/ delta) to limit information leakage. 4. Adaptive Pipeline: detect dataset sensitivity and automatically select/tune methods per-slice. 5. Attack Simulation & Verification: run linkage and inference attacks to validate safety before release.

Ideas Used

- Domain-aware quasi-identifier detection - DP-trained synthetic generators (CTGAN/TVAE with DP-SGD) - Targeted SDC applied only to high-risk slices - Microaggregation and adaptive k-anonymity per slice - Automated optimizer (Bayesian) for privacy-utility tuning - Audit logs and reproducible configuration management

Advantages

- Stronger privacy than simple anonymization: covers identity, attribute and membership attacks. - Higher data utility than blanket generalization by preserving joint distributions and applying targeted perturbations. - Domain-agnostic: works for census, health, finance, and more. - Verifiable: attack simulations and privacy ledger provide auditability for NSO compliance. - Configurable: stakeholders can select privacy thresholds and utility tasks.

Comparison: Existing NSO Method vs SafeData 2.0

Privacy Protection: - Existing NSO: Remove direct IDs; vulnerable to linkage. - SafeData 2.0: SDG + DP + targeted SDC; very low re-identification risk. Data Utility: - Existing NSO: High initially but risky; may be revoked if breaches occur. - SafeData 2.0: High and stable; preserves distributions and predictive performance. Operational Complexity: - Existing NSO: Low - SafeData 2.0: Moderate-to-High (requires ML + privacy engineering)

Prepared for: MoSPI Hackathon - 'Evaluation of Effectiveness of Data Encryption/Anonymisation and Creation of improved Safe Data Tool'