Data Services Network

Backbone for an Integrated Digital Government

Executive Summary

The modern digital state is moving from siloed databases to integrated ‘Data as a Service’ Networks.

This shift is powered by the Once-Only Principle, which ensures citizens and businesses provide information to public administrations only once.To deliver this vision, governments deploy layered architectures featuring blockchain for integrity, distributed exchanges like X-Road, and automated orchestration.

The Once-Only Principle eliminates redundant data requests by allowing authorities to retrieve verified information from authoritative registries—with explicit consent. It cuts administrative burden, reduces errors, and limits unnecessary data collection while respecting privacy.

Defining the Data Services Network: A Blueprint for Digital Government

In the digital age, governments worldwide face a common challenge: fragmented data systems that hinder efficient service delivery, waste resources, and frustrate citizens. Traditional approaches—centralized databases or isolated agency silos—often lead to duplication, security vulnerabilities, and delays.

Enter the Data Services Network (DSN), a forward-looking blueprint for digital government. It reimagines public sector infrastructure as an interconnected, secure, and citizen-centric ecosystem.

At its core, the DSN comprises two interdependent pillars: (i) a robust data exchange platform, such as Estonia's acclaimed X-Road, and (ii) standards for unified citizen records.

Together, these enable seamless, privacy-preserving data sharing while upholding principles like data minimization and citizen consent. The result? A government that operates more like a modern network than a bureaucratic machine—efficient, transparent, and responsive.

The First Pillar: A Secure Data Exchange Platform

The foundation of any DSN is a decentralized data exchange platform that allows government agencies, private sector partners, and even cross-border entities to share information securely without creating a single, vulnerable central repository. Estonia's X-Road, launched in 2001 and now open-source, serves as the gold-standard example.

X-Road functions as a centrally managed but distributed Data Exchange Layer (DXL). Organizations connect via "Security Servers" that handle encryption, digital signatures, timestamps, and access controls.

A lightweight Central Server manages the network's registry and policies, but actual data flows directly peer-to-peer between a service consumer and provider. This architecture guarantees three essentials: interoperability across disparate systems, data integrity (nothing is altered in transit), and confidentiality through transport-layer

encryption and organization/machine-level authentication.

Unlike monolithic databases, X-Road supports real-time queries, large data transfers, and even multi-system searches while logging every transaction for auditability. It powers Estonia's "once-only principle": citizens and businesses provide data just once, after which authorized systems reuse it automatically.

Today, X-Road connects over 1,000 databases and handles tens of millions of monthly inquiries across public and private sectors.

Other nations have adopted or adapted similar platforms (e.g., Finland's Suomi.fi Data Exchange Layer, which links directly with Estonia's), proving the model's scalability for both national and international use.

The Second Pillar: Standards for Unified Citizen Records

A data exchange platform alone is not enough; it requires harmonized standards for unified citizen records to ensure data is meaningful, consistent, and trustworthy when shared. This pillar establishes common frameworks for how citizen information is structured, identified, accessed, and protected—without forcing everything into one giant database.

Key elements include:

- **Unique digital identifiers and authentication:** Every citizen (and often businesses) receives a secure digital ID (e.g., Estonia's mandatory e-ID card or mobile-ID), enabling strong, multi-factor verification across services.
- **Common data schemas and APIs:** Standardized formats (such as JSON schemas or OpenAPI specifications) define fields for personal data—like addresses, health records, or tax information—so systems "speak the same language."
- **Privacy-by-design and consent mechanisms:** Built-in rules enforce granular access controls, data minimization, and citizen consent. Logs ensure traceability, while citizens can view and manage their data usage.
- **Interoperability protocols:** Alignment with global standards (e.g., EU eIDAS for cross-border recognition or NIST digital identity guidelines) allows seamless integration while respecting local laws like GDPR.

These standards create a "unified view" of citizen records on demand. An agency

doesn't store copies of everyone's data; it queries the authoritative source via the exchange platform using verified credentials. This eliminates redundancy, reduces errors, and empowers citizens with control over their information.

Synergies: How the Pillars Create a True Network

The DSN's power lies in integration. The data exchange platform provides the secure "pipes," while unified citizen record standards supply the "contents" in a usable, governed format.

A tax authority, for instance, can instantly verify a citizen's address from the population registry without paperwork—securely authenticated via digital ID and routed through X-Road-like infrastructure. This operationalizes the once-only principle at scale, slashing administrative burdens and enabling proactive, personalized services.

Real-World Impact and Benefits

Countries implementing DSN-like elements have seen dramatic results:

- **Efficiency gains:** Reduced duplication and faster processing (Estonia reports millions of automated exchanges monthly).
- **Citizen satisfaction:** Seamless services—apply once for benefits, vote digitally, or access healthcare records instantly. Public sector digital transformation often yields 80%+ citizen satisfaction and 45% efficiency improvements.
- **Security and resilience:** Decentralized design minimizes breach risks; every transaction is encrypted and auditable.
- **Innovation and inclusion:** Open standards spur private-sector apps, AI-driven insights, and cross-border services while advancing digital equity.
- **Cost savings:** Lower IT maintenance and paperwork; Estonia ranks among the world's top e-governments partly due to X-Road.

The Path Forward: Why DSN Matters Now

The Data Services Network is more than technology—it is a governance model for the 21st century.

As governments pursue AI, open data, and sustainable development goals, the DSN

provides the trusted backbone: secure pipes for exchange plus standardized records for reliability. Nations like Estonia have proven it works; others—from the UK's digital blueprint to emerging Digital Public Infrastructure initiatives—are moving in this direction.

By adopting the DSN framework, governments can move beyond digitizing paperwork to truly re-engineering public service delivery. Citizens gain convenience and control. Societies gain efficiency, transparency, and resilience.

In a fragmented digital world, the Data Services Network offers a unified, future-ready blueprint—one where data serves people, not the other way around.

Data Services - A New Paradigm of ‘Tell Me Once’ Efficiencies

The Once-Only Principle (OOP) represents a fundamental shift in public administration philosophy. Instead of repeatedly requesting the same documents—such as proof of address, income verification, or professional qualifications—authorities retrieve verified data from existing registries with explicit user consent.

This reduces administrative burden, minimizes errors from manual re-entry, and enhances user experience while strengthening data privacy by limiting unnecessary collection and central storage.

In the European Union, the Once-Only Technical System (OOTS), launched in December 2023 under the Single Digital Gateway Regulation, enables cross-border data exchange for 21 key procedures, including professional qualifications recognition and permit applications.

Citizens and businesses simply consent once via an existing public service portal; relevant data flows securely between competent authorities without creating new central repositories or requiring additional apps.

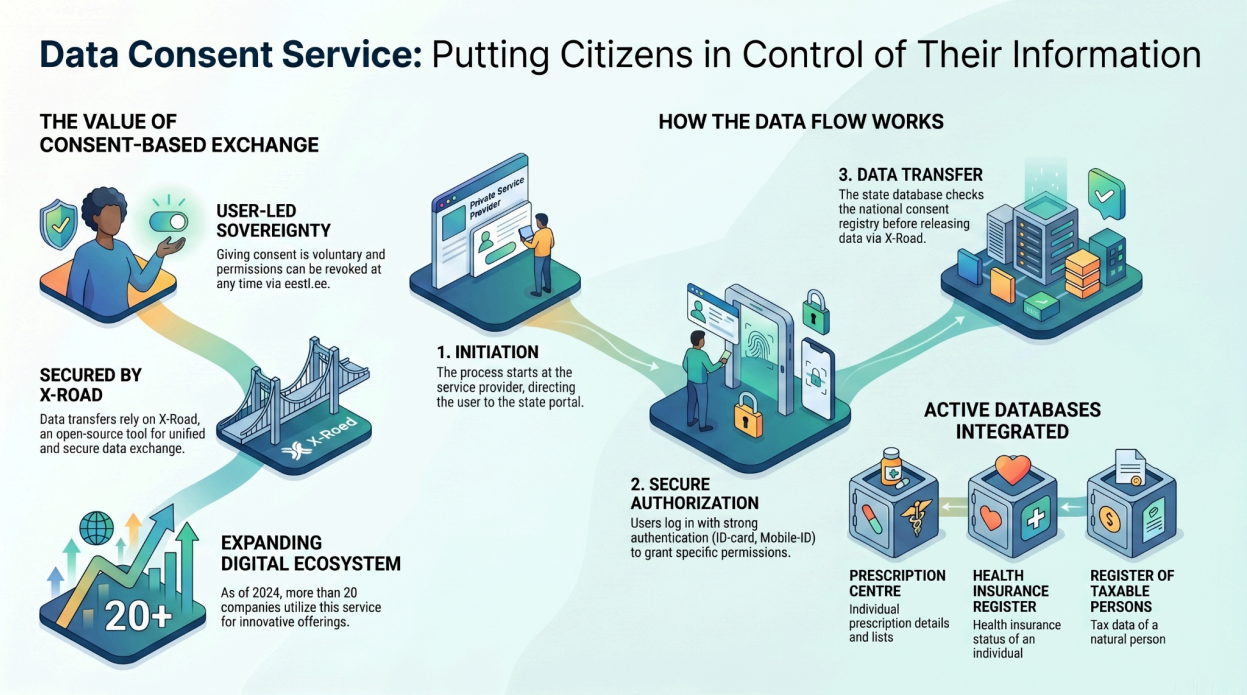
This principle demands robust technical foundations. Siloed systems cannot support it without creating security vulnerabilities or integration nightmares. Enter the DSN: a layered, interoperable infrastructure that acts as the "data highway" of the digital state.

Estonia’s Consent Service

The building blocks of these systems is citizen-controlled data sharing, such as Estonia’s ‘Data Consent Service’, an e-service developed by the Information System Authority which allows a person to give permission to the state to share their personal data with a certain service provider.

With the data consent service, you can allow the transfer of your personal data to companies that offer innovative and personalised services based on personal data. Consents can only be given for the transfer of the data set required for a specific service. After consent has been given, the data held by the state is transferred to the

private company that obtained the consent.



By using the data consent service, you can decide on the processing of your personal data by choosing third parties who can access your data. The use of the data consent service and the giving of consents is always voluntary. Consents can be revoked at any time.

The Magic of "Once-Only": A Guide to the Frictionless State

The "Once-Only" principle represents a paradigm shift in public service delivery. Rather than requiring users to repeat data entry across different departments, the state creates a fluid ecosystem where data is shared and reused under strict security protocols.

- **Reduced Administrative Burden:** Minimizing the time and effort required for citizens to interact with the state during major life events (birth, marriage, bereavement).
- **Process Efficiency:** Streamlining internal government workflows by eliminating redundant record-keeping.
- **Data Integrity:** Ensuring that updates to a "master record" are reflected across

all authorized agencies.

In the traditional bureaucratic model, the burden of data management falls on the individual. If you move house, you must notify the tax office, the health department, and the licensing bureau separately.

The **"Once-Only" Principle (OOP)** flips this script. It is a paradigm shift where citizens and businesses provide information to public administrations exactly once. From that point, the state takes responsibility for the secure internal sharing and reuse of that data.

For a digital transformation architect, the "So What?" is clear: we are moving from a "siloed" bureaucracy—where every department acts as an isolated island—to a **dynamic, fluid ecosystem**. This transition treats the citizen's time as a finite, respected resource rather than an administrative input.

Traditional Model	Once-Only Model
Manual Repetition: Citizens fill out identical forms for every agency.	**Automated Reuse:** Data is provided once and shared via secure protocols.
Siloed Databases: Fragmented records with no synchronization.	**Interconnected Ecosystem:** Real-time updates across the state apparatus.
Reactive Service: The burden is on the user to trigger updates.	**Proactive Governance:** The state anticipates needs based on data triggers.
Manual Verification: Physical documents are required to prove facts.	**Digital Proofs:** Verification happens via secure, machine-to-machine exchange.

This seamless user experience is made possible by a sophisticated "invisible engine" that ensures data moves between agencies with absolute security and legal authority.

The "Tell Us Once" Experience: A Deep Dive into the UK

Model

To see the Once-Only Principle in action, consider the UK's **"Tell Us Once"** service.

This system addresses the administrative complexity of bereavement—a life event where citizens "least feel like doing" paperwork. By informing a single registrar, a family triggers a cascade of notifications to several critical government agencies.

When a death is registered, the registrar provides a unique reference number valid for 28 days. Once authorized, the service notifies several key agencies. Each agency receives the notification and takes a specific administrative action:

- **HM Revenue and Customs (HMRC):** Updates personal tax records and cancels tax credits or child benefit claims.
- **Department for Work and Pensions (DWP):** Ceases state pension payments and updates active benefit records like Universal Credit.
- **Passport Office:** Cancels the deceased's British passport to ensure identity security and prevent fraud.
- **Driver and Vehicle Licensing Agency (DVLA):** Cancels the driving license and removes the deceased as the registered keeper for up to five vehicles.
- **Local Councils:** Updates Council Tax records, cancels Blue Badges, and removes the individual from the Electoral Register.

Users must provide the deceased's date of birth, National Insurance number, and details of their next of kin and executors. Commercial organizations (banks, utility companies) are not notified by this service and must be contacted separately.

Fulfilling the "Once-Only" mandate requires a strategic shift from simple request-response interactions to an **Event-Driven Architecture (EDA)**. In this model, a single administrative trigger—such as a death registration—cascades into an automated series of notifications, drastically reducing the burden on the bereaved.

Data Exchange Platform (DXP)

The foundation of any DSN is a decentralized data exchange platform that allows government agencies, private sector partners, and even cross-border entities to share information securely without creating a single, vulnerable central repository.

X-Road

Estonia's X-Road, launched in 2001 and now open-source, serves as the gold-standard example. The X-Road is a peer-to-peer data exchange ecosystem that connects disparate government systems without a central database of citizen records, serving as the benchmark for secure, distributed exchange.

- **Central Server**: Manages the registry of members and publishes the "Global Configuration" (trusted CAs and security parameters). It never processes actual citizen data.
- **Security Servers (Gateways)**: Mandatory mediators for all calls. They enforce **mTLS** channels, apply digital signatures, and provide time-stamping for non-repudiation.
- **Information Systems**: Internal agency applications that interact with Security Servers via REST or SOAP, abstracting cryptographic complexity.

Estonia's X-Road connects over 900 institutions and enterprises, powering more than 3,000 digital services and saving thousands of working years annually in administrative efficiency. Finland adopted it nationally, and in 2018 the two countries federated their ecosystems—the world's first X-Road Trust Federation—enabling seamless cross-border exchanges of population, business, and tax data.

The model has spread globally: Iceland, the Faroe Islands, parts of Brazil, Germany (for healthcare pilots), and others have implemented or adapted X-Road variants. Its open-source nature (managed by the Nordic Institute for Interoperability Solutions—NIIS) allows customization while preserving core security guarantees.

National Data Hub

Scotland has pioneered an approach described as a ‘National Data Hub’.

This secure online self-service platform—delivered by the Improvement Service—has become a cornerstone tool for data matching and cleansing across Scottish public sector organisations.

Launched as a self-service platform in early 2018, the Data Hub originated from a very practical problem in 2016. Transport Scotland and local authorities needed to replace around one million expired National Entitlement Cards (free bus passes for older and disabled people).

The challenge? Outdated addresses and mismatched records meant many cards were being sent to the wrong people—or not at all—leading to service disruptions, public frustration, and increased administrative costs.

The Improvement Service stepped in to build a dedicated tool that could validate and cleanse large datasets quickly and securely. Today, the Data Hub is a trusted, free service for all Scottish local authorities and partner public sector organisations. It is built on the same secure infrastructure as the widely used mygovscot myaccount system, ensuring high standards of data protection and accessibility.

Data Matching

The system allows local authorities to upload datasets (e.g., customer records from CRM, benefits, housing, or social care systems) and have them automatically matched or enriched with UCRNs from authoritative sources, primarily drawing on NHSCR data.

At its heart, the Data Hub offers a suite of specialised programs that automate what used to be labour-intensive manual processes:

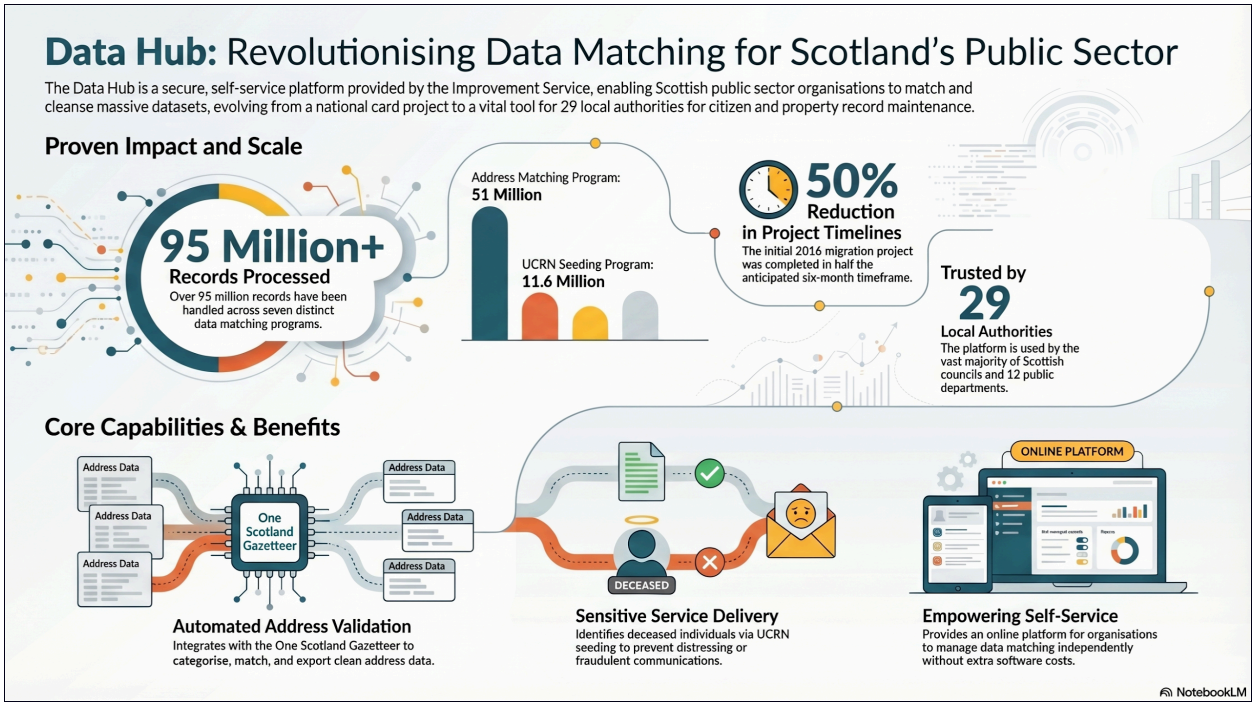
- **Address Matching Program:** The most popular feature. It cross-references submitted address lists against the authoritative One Scotland Gazetteer (OSG) dataset. Users receive categorised results (match, no match, new match needed) and can resolve ambiguities using an integrated interactive map and address search tool. Outputs are downloadable in convenient templates.
- **Unique Citizen Reference Number (UCRN) Seeding Program:** Available to local authorities, this adds or verifies the unique citizen identifier used across

Scottish public services. It can also flag dates of death—vital for benefits audits and fraud prevention.

- Additional programs support seeding missing data, matching records across multiple sources, and generating summary/analysis reports.

The platform is deliberately user-friendly. Users upload their data, start a process, and receive email notifications when results are ready—allowing them to continue other work rather than babysit lengthy batch jobs.

It handles massive volumes: one organisation alone processed 27.8 million records in a single run. Overall, the Data Hub has now processed over 95 million records across seven distinct programs, with the Address Matching tool accounting for more than 51 million.



Real-World Impact: Faster Services, Less Waste, Better Outcomes

The benefits are concrete and measurable. Public sector bodies report:

- **Dramatic time and cost savings:** A project that once took six months can now be completed in three.
- **Improved service accuracy:** Correct addresses prevent cards, letters, or

benefits from going astray. Accurate citizen data supports everything from vaccination cohort identification to energy efficiency programmes.
- **Fraud reduction and better governance:** Flagging deceased individuals helps stop payments to non-existent claimants.
- Strategic value: Organisations use the cleansed data for master data management, customer analytics, and long-term planning.

Twenty-nine of Scotland's 32 local authorities, plus nine other public sector organisations, now rely on it regularly.

Automated Orchestration and Consent Services

Modern GDXPs include orchestration engines that automate workflows: discovering available data sources, routing queries, enforcing access policies, and handling consent revocation.

Semantic interoperability standards ensure data from disparate systems is understandable across borders or agencies. Base registries (authoritative sources for core data like identities, addresses, or company details) feed into this layer, reducing duplication.

Orchestration is the automated coordination of complex workflows across multiple systems. It differs from simple automation by managing dependencies and reacting dynamically to events.

Event-Driven Architecture (EDA)

To implement services like "Tell Us Once," governments must move toward EDA, where an action in one agency triggers a cascade of notifications across the sector.

EDA is a design where systems are "loosely coupled" and only act when they detect a specific "event"—a meaningful change in state, such as a birth or a change of address—allowing government services to respond asynchronously in real-time.

This proactive model feels effortless to the user, but it rests on a technical foundation designed to prevent unauthorized access or data tampering.

- **Event Carried State Transfer (ECST):** Carrying data directly to consumer agencies to decouple services.

- **Orchestration Layer:** A dedicated service (e.g., Apache Kafka) that coordinates interactions between modern cloud components and legacy on-premises systems.
- **"Leave and Layer":** Wrapping legacy systems in API wrappers to allow them to participate in modern event flows without a total rewrite.

Singapore's **MyInfo** platform offers "instant provisioning" by pulling verified government data directly into service applications. Similarly, New Zealand's **SmartStart** integrates services around the birth of a child. In these models, the citizen doesn't just "tell" the government once; the government proactively "knows" and responds.

Under this model, the government uses **Change Data Capture (CDC)** to monitor primary registries for state changes. When an event occurs—like a birth registration—the system utilizes **Event Carried State Transfer (ECST)** to push the necessary data directly to consumer agencies (like tax or social services) without the user ever making a second request.

Governance and Security Overlay

Centralized policy management (e.g., access rights, legal agreements) coexists with decentralized execution. This hybrid model balances sovereignty with collaboration. Additional features often include monitoring dashboards, high-availability clustering, and integration with digital identity systems (e.g., eIDAS in Europe) for strong authentication.

Privacy by Design: Your Data, Your Control

Once-Only technology is the practical implementation of **Privacy by Design**, a requirement under Article 25 of the GDPR. This ensures that privacy is not an afterthought but a core architectural component.

Unified Citizen Records

A data exchange platform alone is not enough; it requires harmonized standards for unified citizen records to ensure data is meaningful, consistent, and trustworthy when shared. This pillar establishes common frameworks for how citizen information is structured, identified, accessed, and protected—without forcing everything into one giant database.

For example by standardising data using trusted identifiers—such as Unique Property Reference Numbers (UPRNs), UCRNs, and Community Health Index (CHI) numbers, Scotland's Data Hub acts as "the missing link" that joins up housing, health, social care, and other services.

UCRN vs CHI: A Comparison of Scotland's Key Citizen Identifiers

Scotland uses two primary unique identifiers for citizens in public services: the Unique Citizen Reference Number (UCRN) and the Community Health Index (CHI) number.

The UCRN is a unique, persistent identifier assigned to individuals in Scotland, typically at birth registration (often linked to the birth registration number) or when they interact with certain government services. It serves as a common reference across public sector databases to enable accurate data linkage without relying solely on names, addresses, or other mutable personal details.

It complements other key identifiers:

- UPRN (Unique Property Reference Number) for addresses/properties.
- CHI (Community Health Index) number, primarily used in NHS Scotland.

The UCRN is managed in connection with the NHS Central Register (NHSCR) and supports broader digital identity initiatives like mygovscot myaccount. Its use is promoted in Scotland's digital strategies for secure, ethical data sharing across health, social care, housing, benefits, and other services.

Both are managed through the NHS Central Register (NHSCR) maintained by National Records of Scotland (NRS), but they serve distinct yet complementary purposes in

enabling secure, accurate data linkage across government and health systems.

- **CHI Number:** This is the unique patient identifier for NHS Scotland. It is the core identifier in the Community Health Index, a population register covering all patients registered with general practices in Scotland (including residents, temporary visitors, and non-Scottish patients). Its primary role is to support healthcare delivery, patient records, GP registrations, prescriptions, hospital admissions, and health data linkage.
- **UCRN:** This is a broader Unique Citizen Reference Number designed for use across the wider public sector, particularly by local authorities and non-health services. It enables consistent identification for services such as housing, benefits, social care, libraries, National Entitlement Cards (e.g., free bus passes), and mygovscot myaccount. It supports joined-up government by acting as a common reference for citizen records outside (or linking to) purely clinical systems.

In essence, CHI is health-sector focused, while UCRN is the cross-government citizen identifier. They are often linked via NHSCR, allowing secure mapping between health and local authority data.

Format and Structure

- CHI: A 10-digit number with embedded meaning:
  - Digits 1–6: Date of birth (DDMMYY).
  - Digits 7–9: Sequence number.
  - Digit 9: Indicates gender (odd for male, even for female).
  - Digit 10: Check digit for validation.
  - Example: Something like 0101011234 (where 010101 is 1 Jan 2001).
- UCRN: A unique persistent number, often derived from or linked to birth registration details. For individuals born in Scotland, it is typically based on the birth registration number. It has no embedded personal details like date of birth or gender, making it more privacy-friendly in that regard. It is assigned or seeded from NHSCR.

Key Similarities

- Both are unique, persistent identifiers for individuals.
- Managed centrally via the NHSCR, which links them and provides matching/seeding services.

- Used for accurate record linkage, de-duplication, and data sharing while complying with privacy principles.
- Support fraud prevention (e.g., date-of-death flagging) and efficient service delivery.
- Available through tools like the Improvement Service's Data Hub for seeding/matching in local authority datasets.

The two are explicitly designed to work together. Strategic frameworks recommend using either CHI or UCRN for health and social care information sharing. NHSCR provides matching services so that a citizen's record in a council system (via UCRN) can be linked to their NHS record (via CHI) without exposing unnecessary data.

Public Health Scotland's CURL (CHI-UPRN Residential Linkage) further extends this by linking CHI to addresses via UPRN (Unique Property Reference Number), enabling spatial analysis and joined-up care between health, housing, and social services.

In the Data Hub, UCRN seeding is a dedicated program for local authorities, while CHI is used in health contexts or as a secondary matcher.

Conclusion: Real-World Impact and Benefits

Countries implementing mature GDXPs report transformative outcomes:

- Efficiency gains — Reduced paperwork, faster service delivery, and lower operational costs. Estonia estimates X-Road contributes significantly to its digital economy, with 99% of public services online.
- Citizen-centric services — Proactive, "no wrong door" government where data follows the user. Cross-border scenarios, such as a Finnish resident accessing Estonian services or vice versa, become frictionless.
- Resilience and sovereignty — Decentralized architecture avoids single points of failure. Data remains in national or organizational control, supporting digital sovereignty amid geopolitical tensions.
- Innovation enablement — Private sector integration opens doors to public-private data ecosystems, powering applications in health, mobility, and finance while respecting privacy.

Challenges remain, including performance overhead from security layers, legacy system integration, varying national legal frameworks, and ensuring equitable adoption across smaller agencies. Performance concerns in some implementations (e.g., additional latency from mandatory security) highlight the need for ongoing optimization.

Emerging Trends and the Road Ahead

As of 2026, GDXPs are evolving toward deeper integration with AI, synthetic data generation for safe analytics, and advanced identity management. Trends include:

- Federated learning and privacy-preserving technologies for collaborative insights without raw data sharing.
- Expanded cross-border data spaces (building on EU OOTS and Nordic models).
- Modular, cloud-native deployments that allow incremental modernization rather than big-bang replacements.
- Stronger emphasis on ethical governance, including transparent auditability and citizen data dashboards showing exactly how their information is used.