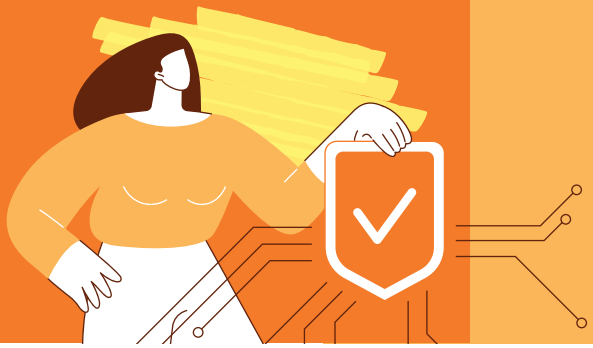


GOVERNANCE EXPLAINER

Sharing Data Safely Across the Public Sector

Safeguard

Lee Kuan Yew School of Public Policy

Institute for GOVERNANCE and LEADERSHIP

Sharing Data Safely Across the Public Sector

In our deeply digital age, governments rely on vast amounts of information to deliver services, make decisions and respond to crises. At a minimum, data sharing fosters coordination and efficiency; at its best, it drives innovation. Meanwhile, safeguarding data through strong protections from unauthorised access, breaches or misuse is essential to preserve the integrity of those benefits.

Why Do Data Sharing and Data Security Matter to Governments?

Data sharing and data security are interdependent: effective sharing requires robust safeguards, and good security enables responsible sharing. Together, data sharing and data security form a foundation for smarter governance and stronger institutions.

Improved Policymaking and Service Delivery

A 2019 OECD report described data as the lifeblood of the "intricate patchwork" of public sector institutions, and data sharing as the beating heart.[1] Linking data from different – and sometimes, seemingly unrelated – areas can enable a more complete and accurate understanding of

people's needs. Services to meet those needs can then become more targeted and responsive rather than following one-size-fits-all prescriptions.

For example, shared profile data could lead to a single mother in a rural village automatically receiving childcare support, a maternal health card and internet subsidies for her child's remote learning. A single health record system that provides general practitioners, hospitals, and social agencies with access to health data could enable the automatic application of subsidies for checkups or fitness programs to eligible individuals based on income and medical history. Governance becomes predictive and personalised, and outcomes accelerated and enhanced beyond their individual parts.

Trust and Legitimacy

Governments can sustain greater trust among citizens by giving them visibility over the use and sharing of their data. Open data platforms or published dashboards enable external scrutiny, public engagement and accountability over data sharing and the policy decisions that arise from it. Meanwhile, data security is central to maintaining public trust in digital government: the secure, ethical and transparent handling of sensitive information increases people's willingness to share it, while breaches undermine confidence and can slow the adoption of innovations. Strong data safeguards help governments signal that they take data protection seriously.

Operational Efficiency

No one wants to do the same work twice. But agencies that operate in silos often collect the same data multiple times and build and maintain separate systems, creating duplicate work for both government and citizens and needlessly reinventing the wheel. Secure data sharing infrastructures direct information to where it is needed and reduce redundancy, paperwork and manual checks. For example, shared databases for eligibility assessment enable agencies to automate cross-checks and detect errors or fraud. Agencies can then reallocate resources that would ordinarily have gone towards these efforts to higher value tasks, leading to cost savings and productivity gains for themselves as well as faster provision of services to the public.

National Resilience

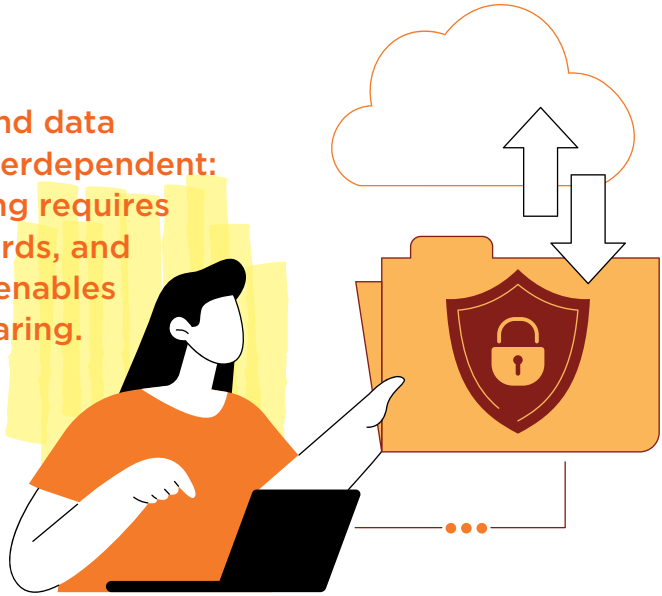
A government's ability to combine speed, coordination and trust through data is a defining feature of national resilience in this era of digitisation. The crises of the last

1 OECD, "Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies", OECD Publishing, 2019, https://doi.org/10.1787/276aaca8-en.

decades – pandemics, natural disasters, cybersecurity events and more – have demonstrated the value of secure, real-time data sharing. No single agency has the full picture necessary to adequately handle a given crisis situation or to anticipate future crises. Data sharing is crucial for a quick and cohesive response, while data security ensures the protection of sensitive data even under emergency conditions. The 2021 ransomware attack on Singapore's Eye & Retina Surgeons medical clinic, for example, triggered a swift, coordinated response across the Ministry of Health, the Cyber Security Agency and the police to strengthen cyber defences and prevent patient data from leaking into the public domain.

Meanwhile, Singapore's government uses a whole-of-government strategy, with multiple agencies collaborating on data sharing, modelling and infrastructure planning, to build resilience against climate change-driven risks of extreme weather events and sea level rise in the future.

Data sharing and data security are interdependent: effective sharing requires robust safeguards, and good security enables responsible sharing.



How Do Governments Share Data Securely?

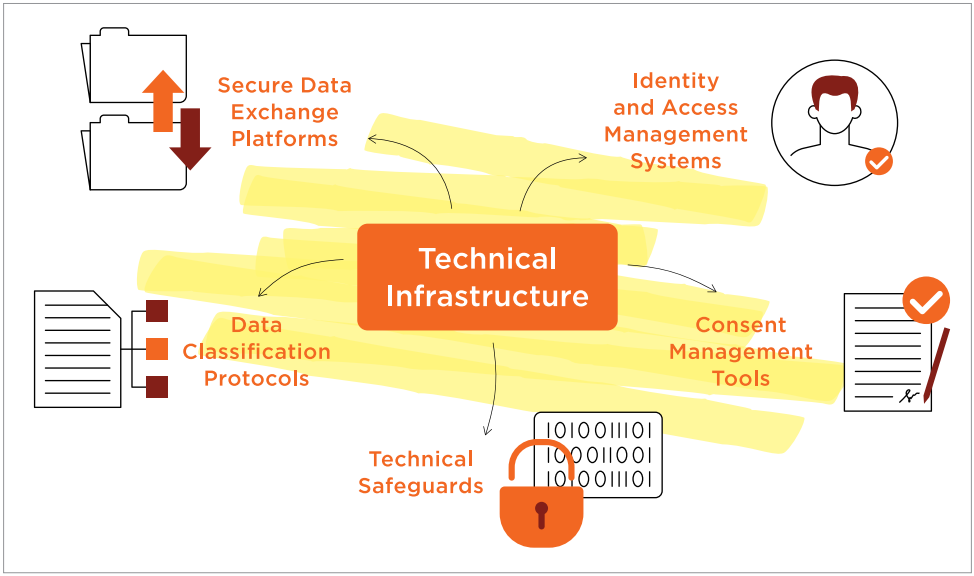
Recognising the value of data sharing and security is just a starting point. How do governments actually put these principles into practice and embed them into public systems?

Technical Infrastructure

Data sharing and security are impossible without robust technical infrastructure. A few key components form the backbone of a digital government capable of managing secure and efficient data flows.

i. Secure Data Exchange Platforms

These systems allow data to move securely between agencies while protecting privacy and ensuring accuracy. For example, Singapore's API Exchange acts like a national electricity grid: instead of laying new cables for every home, agencies simply "plug in" to the platform to access or share data.[2] Built-in access controls ensure that only authorised systems and personnel can retrieve or send data, and that all interactions are logged for auditing and accountability.



2 Medha Basu, "Inside Singapore's plans to share data across agencies", GovInsider, 19 May 2017, https://govinsider.asia/intl-en/article/api-exchange-apex-govtech-chan-cheow-hoe.

ii. Identity and Access Management Systems
These systems form a critical layer of defence in any secure data-sharing ecosystem. They ensure that only verified and authorised users can access specific datasets or digital services, at the right time and for the right purpose. Identity and access management combines user authentication (proving you are who you say you are) and access control (limiting what you're allowed to see or do).

The systems should ideally tailor permissions to roles and responsibilities, preventing unauthorised access to sensitive or classified information. For example, a social services officer might be allowed to view income and household data, but not medical records. If you've ever logged into a service using single sign-on, two-factor authentication, one-time passcodes or biometric scans, you have interacted with identity and access management in action. The growth of hybrid and remote workforces in the post-COVID world has made these systems particularly important, as users now access data from a wide variety of locations apart from their official workplaces.

iii. Data Classification Protocols
Clearly defining different categories of personal data enables governments to make effective decisions around access control, data retention and audit requirements. ISO/IEC 19441, for example, is an international standard that outlines a spectrum of data identifiability levels, from data we can unambiguously associate with an individual to data that only shows overall patterns and includes no individual-level details.[3]

A clear and consistent framework such as this helps governments determine who should have access to what kind of data, under what conditions. For instance, frontline officers might only access pseudonymised data for operational purposes, while analysts might need anonymised or aggregated datasets for their research. Different classes of data may also be subject to different retention periods and security measures such as encryption, access logs or special clearance requirements.

iv. Technical Safeguards
Governments must protect data both in transit (while it is traveling between systems) and at rest (while it is living on servers or devices). Tools that serve these ends include end-to-end encryption, firewalls, backup and recovery systems, Virtual Private Networks and more.

3 OECD, "Enhancing Access to and Sharing of Data".

v. Consent Management Tools

These uphold privacy and enforce public trust in digital governments by allowing individuals to control how the government uses their personal data. For example, Singaporeans can elect whether or not they want to share their MyInfo profile (see "Singpass") to auto-fill forms when interacting with banks and service providers.

Organisational Culture and Skills

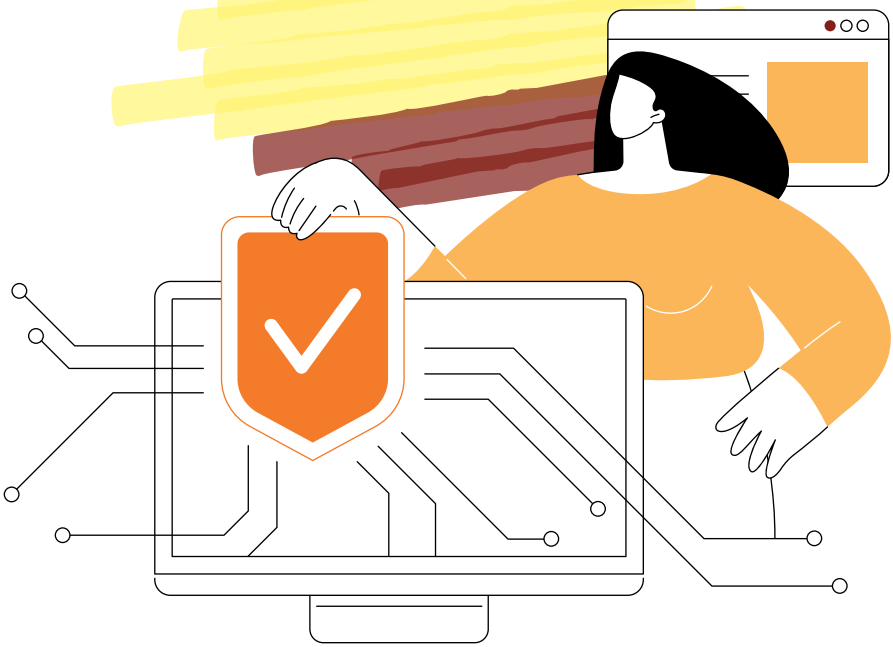
The success of data sharing and data security in government hinges on the people who use and manage data every day. Building a robust data sharing ecosystem requires an organisational culture and human foundation of collaboration, trust and responsible data stewardship across the public sector. This depends on the cultivation of a cross-agency sharing culture. In Singapore, there are rotational postings and joint training programmes that allow civil servants to develop networks, understand how mandates differ across agencies and build a shared sense of purpose. Such initiatives promote systems thinking and encourage a whole-of-government perspective on policymaking and service delivery.

Civil servants should also cultivate a shared language around data – common definitions, classifications and protocols around data use – so that individuals across all domains can talk effectively to each other. Standardised data collection mechanisms across agencies make data easier to share across systems as well as reduce duplication and data cleaning work. To ensure leadership in shaping sound data strategy and ensure compliance with evolving security and privacy standards, agencies might appoint dedicated staff for data governance: Chief Data Officers, Chief Information Officers, privacy experts and data governance managers.

Governance and Frameworks

Data sharing and security in government rely on frameworks, laws and regulations that determine how the public sector can access, use, protect and retain data. The Singapore government, for example, developed the Digital Government Blueprint to guide the government's vision to achieve sophisticated digitalisation within government and provide seamless digital experiences for citizens. Meanwhile, laws such as the Public Sector (Governance) Act 2018 provide strict protocols for data handling and confidentiality within the public sector.

Civil servants should also cultivate a shared language around data – common definitions, classifications and protocols around data use – so that individuals across all domains can talk effectively to each other.



What Challenges Might Governments Face in Data Sharing and Data Security?

Even with well-designed infrastructure, organisational norms and regulatory structures, challenges abound in sharing and protecting data in government, especially as technologies and data practices continue to evolve.

Lack of Resources

The funding, expertise and infrastructure required to securely process, manage, store and merge data, as well as keep that data compliant with data privacy laws, are substantial. These activities are especially critical in high-stakes scenarios such as disaster response or public health emergencies, where real-time data flows can be crucial for informed decision-making and timely action. Governments

Yet technical fragmentation is only part of the challenge. Even when well-meaning policy exists, inconsistent interpretation across agencies can undermine implementation.

often struggle to keep pace with the rapidly evolving demands of modern data systems, particularly when it comes to investing in advanced cybersecurity measures, scalable cloud infrastructure and skilled human capital to manage it all. Inadequate resourcing can lead to outdated systems, fragmented data environments and vulnerabilities in compliance with complex and ever-changing data privacy regulations. Absent sufficient investment, public sector organisations risk falling behind on interoperability, delaying response times and exposing sensitive information to potential breaches.

Fragmented Systems and Inconsistent Interpretation

Efficient data sharing becomes more difficult when different organisations, and even different teams within a single organisation, utilise different data cloud storage systems, data collection methodologies, terminologies and security protocols. These disparities can lead to data silos, integration difficulties, inconsistent data quality and heightened security risks, ultimately hindering seamless collaboration and decision-making. Data themselves are heterogenous and can require different handling mechanisms: for example, governments need to more closely and thoughtfully govern access to personal data than non-personal data.

Yet technical fragmentation is only part of the challenge. Even when well-meaning policy exists, inconsistent interpretation across agencies can undermine implementation. A case in point: in 2024, Singapore's Ministry of Digital Development and Information issued a circular instructing agencies to stop using masked National Registration Identity Card (NRIC) numbers. The circular lacked sufficient clarity and precision for some agencies: for example, it was unclear whether the continued use of NRIC numbers in an Accounting and Corporate Regulatory Authority's tool counted as an "existing" or "planned" use. Despite multiple email exchanges between the ministry and authority, misunderstandings persisted and led to the disclosure of full NRIC numbers on a government portal. A subsequent review suggested that clearer policy articulation and more proactive two-way engagement would have helped to prevent confusion.[4]

Legal Complications

Data sharing and data security are dynamic, and the legal and regulatory landscape has to adapt quickly to keep up.

4 Government of Singapore, "Report of the Review into the Public Disclosure of Full NRIC Numbers on Bizfile People Search", February 25, 2025, https://www.pmo.gov.sg/-/media/PMO/Newsroom/Attachments/20250303-Review-into-the-Public-Disclosure-of-Full-NRIC-Numbers/Report-of-the-Review-into-the-Public-Disclosure-of-Full-NRIC-Numbers-on-Bizfile-People-Search27-Feb.ashx.

Laws and regulations can greatly limit how stakeholders can access, share and use data. Further, the complexity and variability of legal frameworks, especially across jurisdictions, can greatly slow down data flows between and within organisation. Organisations must often navigate a patchwork of regulations that may have overlapping, conflicting or ambiguous requirements. The need to interpret dense legal language and implement tailored compliance mechanisms can introduce substantial delays and friction in the flow of data within and between organisations.

Privacy Breaches

Increased data usage inherently raises the risk of digital security incidents. Personal data breaches can bring huge costs to any data sharing enterprise. These include compromised functioning of essential services, individual harms such as identity theft, loss of confidence in digital services (see "Public Sentiment") and debilitating hits to organisations' reputation, all of which can have knock-on effects on further innovation and investment. The risk of data misuse can be particularly high in external data sharing.

Public Sentiment

Public perception plays a critical and often underestimated role in shaping the landscape of data sharing and security within governments. Data has become a political and cultural issue for governments to navigate. Citizens can be cautious about sharing their personal information, fearing surveillance and other misuses. This public wariness can lead to slower adoption or even avoidance of innovations and digital programs such as digital ID cards or health tracking apps, and high expectations for transparency over the methodology, purpose, nature and protections of data collection.

For example, Singaporean authorities caused a stir when they announced in Parliament that the police could access data from the TraceTogether programme, a Bluetooth-based system for identifying and logging close contact between people during the COVID-19 pandemic, to aid in criminal investigations. Many Singaporeans responded to this announcement with anger. Some stopped using the app or disabled their phone's Bluetooth function. The authorities officially acknowledged their error, and the Singapore Parliament passed a bill explicitly limiting police access to TraceTogether data only for very serious criminal offences, including terrorism, murder and kidnapping. But damage was done: the episode sparked a spike in public demand for data deletion, with 1,155 users applying to opt out of TraceTogether four months after the revelation.[5]

5 Hariz Baharudin, "More than 1,100 users have deregistered from TraceTogether: Vivian", *The Straits Times*, 11 May 2021, https://www.straitstimes.com/singapore/more-than-1100-users-have-deregistered-from-tracetogether-vivian.

How Does Singapore Implement Data Sharing and Security?

The examples above highlight how even a digitally advanced public sector such as Singapore's is not immune to challenges in data governance. These serve as reminders that getting data sharing and data security right is not straightforward, even in well-resourced environments.

Nevertheless, Singapore's public sector remains a leader in many aspects of digital governance. The three initiatives below represent some of Singapore's most advanced and widely adopted examples of digital services that integrate data sharing with strong data security practices. Each system reflects a mature approach to managing sensitive information while maintaining public trust through transparency, encryption and user control.

Singpass

Singpass, Singapore's national digital identity platform, is a cornerstone of the government's approach to secure and seamless data sharing. The system provides personal biometric or SMS authentication for over 2,700 services spanning 800 government agencies and businesses such as banks and healthcare providers and operates on a consent-based model.

A key feature of this model is MyInfo, a data-sharing platform that consolidates personal data from government databases such as the Inland Revenue Authority, the Immigration and Checkpoints Authority and the Central Provident Fund. It enables users to pre-fill application forms and avoid repeating the same information across platforms – but only with their explicit consent. For example, an individual might give their consent for MyInfo data to pre-fill a credit card application form with the relevant government-verified personal information. End-to-end encryption and rigorous cybersecurity protocols and

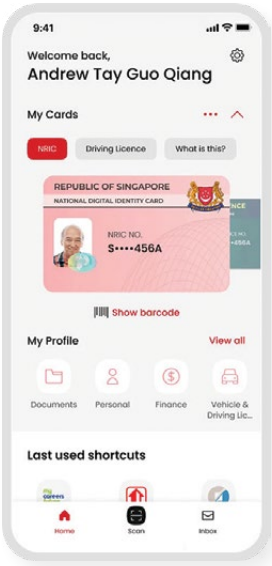


Image credit: Singpass

auditing mechanisms protect all data transfers, giving rise to an ecosystem of high-quality, consistent data that safeguards individual privacy.

LifeSG

The mobile application LifeSG leverages the Singpass digital identity to provide an integrated experience for accessing government services such as registering a child's birth, booking public facilities and enlisting for National Service. MyInfo and Singpass work together to collect and authenticate verified personal information that enables the tailoring of government services to a person's needs and eligibility. For example, LifeSG might highlight vaccination schedules to new parents, training courses to jobseekers or utility bill subsidies to low-income households. The app inherits the Singpass standards of user consent, data security and privacy controls and, like Singpass, helps users avoid entering the same information on multiple platforms.

National Electronic Health Record (NEHR)

The NEHR is a centralised, secure system that compiles key summary health information, including data such as allergies, laboratory test results and medication history, from healthcare providers across the country. Launched

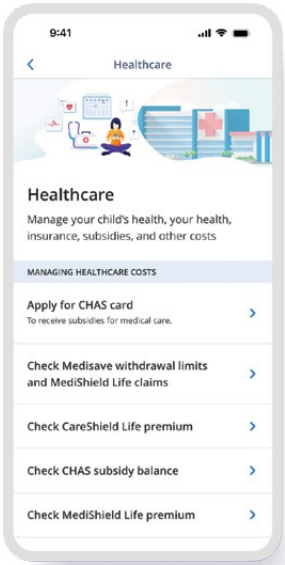
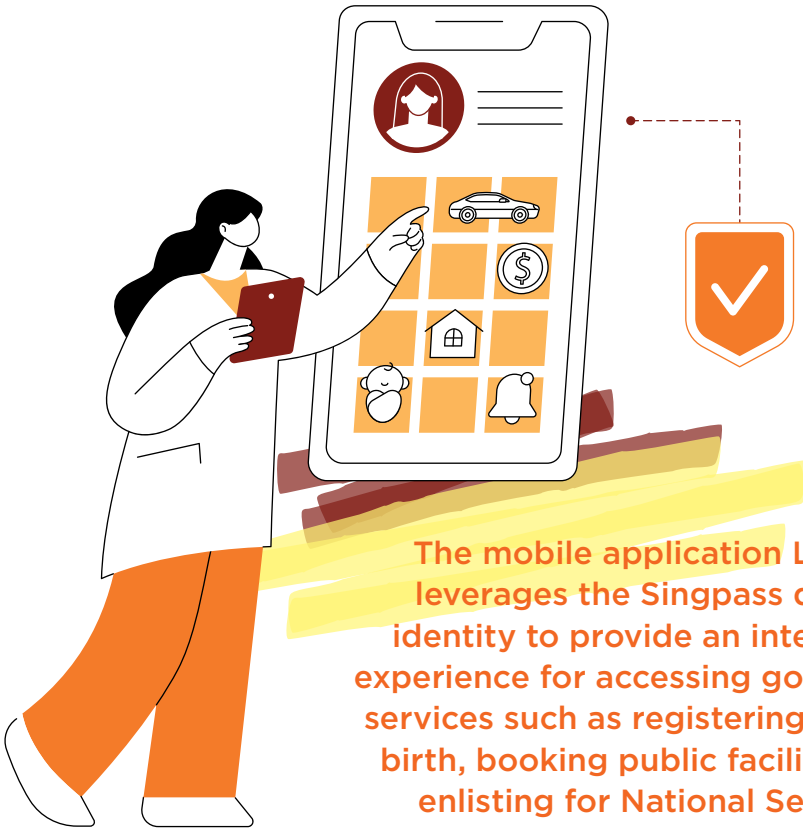


Image credit: LifeSG



The mobile application LifeSG leverages the Singpass digital identity to provide an integrated experience for accessing government services such as registering a child's birth, booking public facilities and enlisting for National Service.

in 2011, the NEHR aimed to support Singapore's vision for "One Patient, One Health Record", in which every patient has a single, unified health record from which clinicians can derive relevant information that they then use to deliver healthcare more seamlessly.

All public healthcare institutions have access to NEHR, while private healthcare institutions are progressively joining the system following a move to make NEHR participation mandatory for all clinics and hospitals. Patients can opt out of allowing access to their data on the NEHR. To ensure data security, the NEHR uses two-factor authentication and conducts regular audits to ensure compliance and detect unauthorised activities. Unauthorised access or misuse of NEHR data is a chargeable offence under the Computer Misuse Act.

Lee Kuan Yew School of Public Policy

Institute for GOVERNANCE and LEADERSHIP

Scan to visit Lee Kuan Yew
School of Public Policy Website