PANEL 6 | SESSION 06

GOVERNED BY TRUST

Data Security and Governance in Healthcare

MODERATOR

Dilpreet Singh — Founder & CEO, Juvoxa; Partner & JAPAC Head, Consulting Services, Singapore. Digital health innovator with deep expertise in Asia-Pacific healthcare technology markets; specialist in health-tech venture development and regional market strategy for digital health platforms.

PANELISTS

1. **Arun Khanna**: Director, Karbir Asia; Former Asia President, Dun & Bradstreet. Extensive experience leading businesses across Asia in FMCG, data analytics, and impact consulting; regional and global roles at P&G, Cabot, Nestlé, and Johnsonville; advisory board member for multiple non-profit organisations.
2. **Krishna Bhaskar**: IAS Officer (2012 Batch); Chairman & Managing Director, TGTRANSCO, Telangana. Oversees electricity transmission for nearly 40 million consumers in Telangana. Recipient of the Prime Minister's Award for Excellence in Public Administration (2019, 2020). Holds degrees from IIT Kharagpur, ISB, and MIT (Applied Economics); Fulbright-Nehru Scholar; Robert Solow Fellow (MIT); World Bank Governance Analytics Fellow (2025).
3. **Vivek Choudhary**: Assistant Professor, Nanyang Business School, NTU Singapore; Former Consultant, McKinsey & Company. Research at the intersection of behavioural operations and digital health platforms; led data-driven health projects for Singapore and Indian government bodies; PhD from INSEAD.
4. **Abhishek Mishra**: Associate Vice President, Digital Health Transformation & Innovation, iKure Techsoft. 10+ years in AI-driven health solutions; worked with India's National Health Authority and global organisations including PATH; leads digital health strategy and large-scale implementation at iKure.

1 PANEL OVERVIEW

Panel 6 examined the critical role of data governance, security, and trust in enabling responsible and effective healthcare systems. As health systems increasingly rely on digital tools, analytics, and data-driven decision-making, the session explored how to balance data utility with privacy, accountability, and social legitimacy.

The discussion united perspectives from data science, public policy, healthcare operations, and community-level implementation. A shared recognition throughout was that while data holds transformative potential for healthcare delivery and public health planning, its misuse or

mismanagement carries serious consequences — eroding trust and producing real harm to the communities it is meant to serve.

A central argument of the session was that healthcare data systems must be designed not only for efficiency and insight, but for ethical integrity, transparency, and public acceptance. The panel framed data governance as a foundational pillar of future health systems — requiring careful alignment between technology, policy, and societal expectations.

2 CONTEXT AND KEY ISSUES

The accelerating digitisation of healthcare has generated an unprecedented volume of data across clinical care, supply chains, insurance systems, and public health surveillance. Yet this data remains largely fragmented across siloed systems — making meaningful integration and analysis difficult, and undermining the very potential it is meant to unlock.

Several interconnected issues were identified as central to this challenge:

- Data quality over data volume: The core challenge is not the absence of data or analytical tools — it is the quality, structure, and usability of existing data. Poorly structured or inaccurate inputs produce flawed insights, reinforcing the principle of Garbage In, Garbage Out.
- Interoperability gaps: Hospitals, insurers, public health programmes, and supply chain platforms operate in parallel silos, with limited capacity to exchange or integrate data. Bridging these gaps requires significant financial investment, technical coordination, and standardisation of data formats.
- Privacy and consent risks: Greater data interconnection amplifies exposure risks. As healthcare data becomes more detailed and linked, the likelihood of misuse, breaches, or unintended disclosure of sensitive information rises correspondingly.
- Context-specific governance needs: Legal, cultural, and political factors vary substantially across countries, meaning that data governance frameworks cannot be universally applied — they must be designed for local context and institutional capacity.

3 INSIGHTS FROM THE DISCUSSION

Data Quality, Purpose, and Leadership

Effective data systems depend on three interrelated components: data quality, analytical models, and data leadership. Even the most sophisticated algorithms cannot compensate for poor-quality inputs or poorly defined objectives.

The panel drew a critical distinction between “searching” for patterns and “finding” answers to specific questions. Purpose-driven data use — where collection is guided by clearly defined problem

statements — consistently generates more actionable insight than broad data harvesting. Organisations must move from accumulating data to deploying it with intent.

Interoperability and Integration Challenges

Integrating multiple datasets remains one of the most technically and ethically complex challenges in healthcare data systems. Differences in data formats, collection frequency, and aggregation levels create significant barriers to combining information effectively.

While integration can unlock powerful insights — such as linking clinical outcomes with supply chain data or population health trends — it simultaneously raises concerns around security and privacy. Strong encryption and siloed storage protect sensitive information but may constrain comprehensive analysis. The panel emphasised the need for balanced approaches: anonymisation, controlled-access systems, and secure data-sharing protocols that enable integration without compromising protection.

Governance Trade-offs and the Data Trilemma

A major conceptual contribution from the panel was the articulation of a governance trilemma: the simultaneous tension between three competing priorities that policymakers must actively navigate.

- Security: Protecting data from breaches, misuse, and unauthorised access.
- Institutional Accountability: Ensuring transparency and clear responsibility across the data lifecycle.
- Social Legitimacy: Building and sustaining public trust and acceptance of data systems.

Achieving all three simultaneously is structurally difficult, and trade-offs are inevitable. Highly centralised systems may deliver strong security and accountability, but risk undermining public trust. Decentralised systems may enhance legitimacy but complicate enforcement and coordination. Systems with strong oversight may build trust over time, but reduce operational speed and flexibility.

This framework makes clear that data governance is not a technical problem with a universal solution — it is a contextual political and institutional challenge requiring deliberate choices.

Consent, Transparency, and Community Trust

The panel placed substantial emphasis on the importance of meaningful, informed consent in healthcare data systems. In many real-world settings — particularly community health programmes — consent is treated as a procedural formality rather than a genuine process of understanding and agreement.

Frontline workers routinely collect sensitive data from communities, often without individuals fully understanding how it will be used. This creates serious ethical risks and erodes the trust that underpins participation. The panel identified three non-negotiable properties of effective consent:

- Transparent: Clearly explaining why data is collected and how it will be used.
- Specific: Linked to defined purposes rather than broad or open-ended usage.
- Revocable: Allowing individuals to withdraw consent at any point.

Digital tools can strengthen consent mechanisms in practice — enabling real-time notifications, audit trails, and user-controlled data access systems that make consent visible and enforceable.

Global Perspectives on Data Governance

Data governance frameworks vary significantly across countries, shaped by historical, political, and cultural contexts. Some regions have developed stringent regulatory frameworks driven by privacy concerns; others have prioritised data sharing for innovation and system efficiency; still others have pursued balanced models that integrate datasets across providers while strengthening safeguards and oversight.

These variations confirm that there is no universal model for healthcare data governance. Systems must be adapted to local institutional capacity, legal environments, and societal expectations — while drawing on international best practice and shared principles.

Data for Policy and System Design

The panel illustrated how large-scale data analysis can generate strategic insights for health system planning — including identifying patterns in patient-provider interactions, workforce dynamics, and service utilisation trends.

Participants cautioned, however, that statistical significance does not automatically translate into policy relevance. Data must be interpreted within its context, with careful attention to potential confounders and system-level implications. Misleading conclusions drawn from technically valid data are a real and underappreciated risk.

4 CHALLENGES IDENTIFIED

The panel identified several persistent barriers to effective healthcare data governance:

- Data quality deficits: Poor structure, inconsistent standards, and inaccurate inputs undermine the reliability of analytics and decision-making.
- Fragmented and siloed systems: Limited interoperability across hospitals, insurers, public health programmes, and supply chains prevents meaningful data integration.
- High integration costs: Combining datasets across systems requires significant financial investment and sustained technical coordination.
- Weak consent mechanisms: Real-world consent practices remain largely procedural, failing to meet the standards of transparency, specificity, and revocability that ethical data use demands.
- Privacy-utility tensions: Protecting sensitive data and enabling powerful analysis remain in structural tension, with no simple resolution.
- Accountability gaps: Responsibility for data quality, security, and ethical use is often unclear or diffuse across the data lifecycle.

- Public trust deficits: Limited transparency in how data is used erodes community confidence in data-driven health systems.
- Jurisdictional complexity: Rapidly evolving and divergent regulatory environments across countries create compliance uncertainty and hinder cross-border data collaboration.

These challenges underscore the need for governance frameworks that simultaneously address technical, ethical, and institutional dimensions.

5 OPPORTUNITIES AND PROPOSED SOLUTIONS

The panel identified clear pathways to strengthen data governance across healthcare systems. Each represents an actionable area for investment and reform:

Data architecture and standardisation: Invest in structured data collection, storage, and sharing frameworks that enable interoperability and analysis. Common data standards and digital infrastructure are the foundation of any effective governance system.

Strengthened consent frameworks: Design simple, transparent, and user-friendly consent systems supported by digital tools. Features such as data access dashboards, usage notifications, and opt-out mechanisms can empower individuals to control their own data and strengthen trust.

Context-specific governance models: Develop governance frameworks that deliberately balance security, accountability, and legitimacy in accordance with local societal expectations and institutional capacities. Policymakers must make trade-offs explicit — and design systems that can adapt as contexts evolve.

Data leadership and capacity-building: Train stakeholders — across health system roles — in data ethics, privacy regulation, and analytical methods. Strong data leadership at institutional level is as important as technical infrastructure.

Transparency as a trust instrument: Clearly communicate to communities and individuals what data is collected, why it is collected, and how it will be used. Transparency is not only an ethical requirement — it is a practical tool for building the public confidence on which data-driven healthcare depends.

6 KEY TAKEAWAYS

- Data is a powerful enabler of healthcare improvement — but its value depends entirely on quality, structure, and purpose-driven use.
- Effective governance requires balancing three competing imperatives simultaneously: security, institutional accountability, and social legitimacy — the Data Trilemma.
- Interoperability and integration are essential capabilities, but must be pursued without compromising data protection or individual privacy.
- Consent must be meaningful, transparent, and revocable — not a procedural checkbox. Communities must genuinely understand how their data is used.

- Public trust is the infrastructure of digital health. Without it, even technically sound data systems will fail to achieve adoption or impact.
- Data insights must be contextualised carefully. Statistical significance alone does not equal policy relevance or practical utility.

7 IMPLICATIONS FOR FUTURE HEALTH SYSTEMS

Panel 6 made clear that trust must be treated as core infrastructure for all data-driven health systems — not an afterthought to technical design. As health systems deepen their reliance on digital technologies and analytics, governance frameworks must evolve in parallel: ensuring data is used responsibly, transparently, and in ways that communities can hold institutions accountable for.

Future health systems must prioritise integrated data ecosystems, robust privacy protections, and genuinely transparent governance mechanisms. Digital infrastructure investment must be complemented by policy reform that promotes accountability, inclusivity, and sustained public engagement. The Data Trilemma — balancing security, accountability, and legitimacy — will require ongoing, context-specific governance choices rather than one-time technical solutions.

Ultimately, data governance is not a technical challenge. It is a societal one. By aligning technology, policy, and public trust, health systems can harness the full potential of data to improve outcomes while safeguarding the rights and dignity of every individual whose information underpins those systems.

> “Trust is not a by-product of good data governance — it is the foundation. Health systems that earn and sustain public trust in how they use data will define the next era of equitable, effective healthcare.”
>
> **— Panel 6 Closing Statement — Workshop Proceedings**