

Data Sovereignty & Patient Privacy in Cloud-Native Healthcare

Rasindu Randheera Gamlath

GM/BSCSD/CMU/06/09

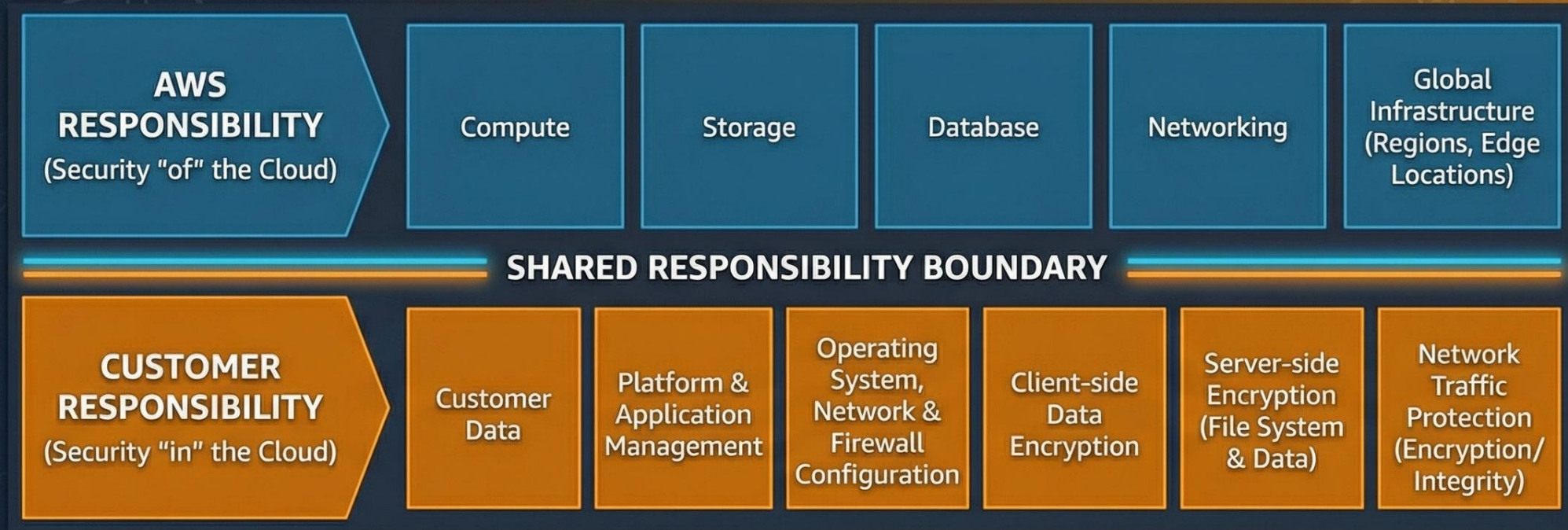


Where Does the MRI Go? The Conflict.

- Massive Digital Footprint & Cloud Migration
- AWS holds the largest share of the global healthcare cloud market.
- Conflict: Technical Speed of Cloud vs. Ethical Necessity of Privacy.



AWS Shared Responsibility Model: The Security Gap



Thesis: Without a Zero-Trust architecture, we risk commodifying human suffering.

Argument: Relying on default vendor security is negligence.

We are Commodifying Human Suffering

- **Informed Consent:** Fluidity in the cloud blurs static consent (Kolaventi, et al., 2024).
- **Secondary Use:** Aggregated data trains proprietary AI models, risking 'data commodification' (Shuaib, et al., 2021).
- **The Gap:** Protection is contractual, needs to be mathematical (stripping patient agency)

When Misconfiguration Becomes Negligence

- **Data Sovereignty:** Cross-Region Replication risks violating rulings (e.g., Schrems II).
- **Shared Responsibility:** AWS secures the cloud; the healthcare provider secures the data in the cloud (Amazon Web Services, Inc, 2025).
- **The Gap:** Technical misconfiguration becomes legal negligence.

Outsourcing Our Professional Ethics

- **Professional Duty:** Failure to implement Client-Side Encryption for PHI is professional incompetence.
- **Vendor Lock-in:** Binding lifetime patient history to short-term vendor contracts is a failure of stewardship (Jukka Varelius, 2008).
- **The Gap:** We trust the network implicitly, 'outsourcing' our professional ethics.

Engineering Exclusion into the Source Code

- **Digital Divide:** Cloud-Native systems require high-bandwidth/low-latency connections.
- **Social Inequality:** Creates a 'two-tier' healthcare system (Nasrulddin, et al., 2025).
- **The Gap:** Architecture is too dependent on connectivity, contradicting the ethical principle of Justice.



What Are the Recommendations?

Don't Trust the Perimeter. Verify Everything.



Action

Verify every request, assuming the network is compromised.



Rationale

This aligns with the professional duty of care (Valanarasu, 2024).



Outcome

Moves security from the 'border' to the 'data' itself.



Zero Trust

Zero Trust Security Model.

Securing Data Mathematically



Action

Implement Homomorphic Encryption.



Example

De-identify medical images before they touch the AI model (Tanksali, et al., n.d.).



Rationale

Allows computation on encrypted data.



Outcome

Satisfies Data Sovereignty by keeping raw data local.

Decouple Intelligence from Connectivity



Action

Design for Offline-First capability.



Strategy

Applications must cache data locally (Baddam, 2025).



Outcome

Ensures equality of access to cloud intelligence regardless of rural connectivity.

Ethics as a Catalyst for Career Growth



Decision Making

Write code that
'protects' human
rights, not just
'works'.



Accountability

Maintain
Professional
Integrity.



Career Growth

Master 'Privacy by
Design' for leadership
roles in governance.

References

- Amazon Web Services, Inc, 2025. Applying the AWS Shared Responsibility Model to your GxP Solution. [Online] Available at: <https://aws.amazon.com/blogs/industries/applying-the-aws-shared-responsibility-model-to-your-gxp-solution/> [Accessed 09 02 2026].
- Baddam, B. R., 2025. Bridging the Digital Divide with CloudBased Automation. European Journal of Computer Science and Information Technology.
- Jukka Varelius, 2008. Ethics Consultation and Autonomy. Springer Nature Link, Volume 14, pp. 65-76.
- Kolaventi, S. S. et al., 2024. Ethical and Privacy Challenges in Cloud-Based Health Informatics for Digital Health Records. Seminars in Medical Writing and Education, 3(Vol. 3 (2024): Seminars in Medical Writing and Education), p. 511.
- Nasrulddin, V., Al-Solmi, J. J., Baobaid, K. K. & Alotaibi, E. M., 2025. The Digital Divide in Healthcare: How Technology. International Journal of Multidisciplinary Research and Publications, 8(1), pp. 279-285.
- Shuaib, M., Alam, S., Alam, M. S. & Nasir, M. S., 2021. WITHDRAWN: Compliance with HIPAA and GDPR in blockchain-based electronic health record. Materials Today: Proceedings.
- Tanksali, S., Fu, S., Gaonkar, A. & Shaik, J., n.d. PixelGuard: Advancing healthcare data privacy through AI-driven de-identification system for medical imaging research. [Online] Available at: <https://aws.amazon.com/blogs/publicsector/pixelguard-advancing-healthcare-data-privacy-through-ai-driven-de-identification-system-for-medical-imaging-research/> [Accessed 12 02 2026].
- Valanarasu, D. P., 2024. Secure and Compliant Cloud Migration Strategies for E-Commerce. Journal of Information Systems Engineering and Management, 1(9), pp. 2468-4376.