Security Analysis of Federated Learning in Healthcare

Policy Proposal

1. Why This Matters

There has been significant promise in integrating AI into healthcare to improve patient welfare[1], whether in early identification of illnesses or specialised healthcare. In medical imaging alone, there have been applications found in tumour detection in oncology[2], genomic characterization[3], tumour subtyping[4], grading prediction[5], outcome risk assessment[6, 7] or chest X-ray analysis[8]. However, based on the results in Section 4, it is evident that AI systems are not fully secure. These models may be poisoned to produce skewed results (Section 4.1), or the training data could be leaked (Section 4.3) or even fully reconstructed (Section 4.2). This could reduce trust in AI systems, limiting the extent of research possible. To encourage further research in this area, AI systems should be designed to be more secure.

As more healthcare data is kept in electronic records, individual medical data could be sold as commodities if hacked. Marketers could potentially tailor medical advertisements based on personal health information; companies might use employee data to justify discrimination. In more extreme scenarios, governments could misuse sensitive medical history, such as records related to HIV status or abortion care, for targeted surveillance.

Furthermore, in medicine, doctors have the right to a patient's data for research or big data analysis only after the patient has provided informed consent, that is, they are fully aware of the condition, treatment risk and benefits, and how the data will be used. However, to transform personal health information into high-quality medical data that can be used as a production factor, it is usually necessary to go through multiple levels of acquisition, analysis and use, with multiple institutions (including medical institutions, companies, public health departments, etc.) jointly participating in it. This gradually weakens each individual's control over the subsequent transformation and derivation of their own health information into big data. The difficulty of implementing and enforcing the principle of informed consent increases layer by layer.

As security practices have been found to affect the latency of the model (from 3-7× for homomorphic encryption, and up to 2× in Section 4.2)[9, 10, 11], researchers must also strike a balance between data privacy and AI performance. Recent political changes have also shown the fractured state of regulation in AI[12], requiring politicians to achieve a consensus to encourage future research. Therefore, the following proposal aims to establish regulations to ensure greater peace of mind and consensus for higher ethical standards when using patient data for research.

2. Current Landscape

2.1 Key Challenges

Within most medical research, the option to opt out must be included. However, while AI companies such as OpenAI claim to comply with the right to erasure, it is unclear how this is achieved because personal information may be contained in multiple forms in AI. This increases the complexity of identifying and isolating specific data points in the latent space of the model. Simply deleting data from a training dataset is a superficial solution, as training data may still be extracted from associated information encapsulated within the model's parameters. It is also unfeasible to retrain models for every data removal request. This undermines the integrity of the deletion process and perpetuates potential privacy violations[13].

In addition, medical research laws may follow the data minimisation principle, where data controllers should collect personal data only as relevant and necessary for a specific purpose. However, limiting the amount of data available for analysis could significantly restrict the accuracy of medical AI, which could produce stress on patients in the event of misdiagnoses[14].

Furthermore, current security practices rely on data anonymisation techniques, where identifiable patient data is replaced with ID numbers or otherwise encoded. However, there is no standardised set of recommendations on anonymising clinical trial datasets, and researchers in clinical trials still consider that anonymisation techniques alone are insufficient to protect patient privacy[15]. Some organisations continue to rely on outdated anonymisation methods, such as k-anonymity and l-diversity, despite their well-documented vulnerabilities[16, 17, 18].

2.2 Policy Case Studies

Privacy laws can differ significantly between countries. The following are a few examples of current regulations on data usage.

2.2.1 Singapore

According to a medical researcher, personal data is fully anonymised with a detailed data management plan, after patient consent. The patient data generally comes from hospital medical records, so companies that participate in research and handle patient data will have to sign NDAs. However, if the anonymisation is reversed, ethics review boards do not factor in, as the data has already been consented to be released.

Privacy protection relies on oversight by hospital ethics committees and the ethical review processes of academic journals. Those boards follow regulations outlined in the Personal Data Protection Act (PDPA)[19] by the Infocomm Media Development Authority (IMDA). The government agency IMDA oversees the responsible adoption of AI across both public and private sectors. The Personal Data Protection Commission (PDPC), a commission within the IMDA, regulates data privacy.

The government has developed various frameworks and tools to guide AI deployment and promote the responsible use of AI, including:

- The Model AI Governance Framework (2020) provides detailed guidance to private sector organisations to address key ethical and governance issues when deploying AI solutions
- AI Verify2, an AI governance testing framework and toolkit designed to help organisations validate the performance of their AI systems against AI ethics principles through standardised tests.
- The National Artificial Intelligence Strategy 2.03 (2023) outlines Singapore's ambition and commitment to building a trusted and responsible AI ecosystem

However, currently, there are no specific laws in Singapore that directly regulate AI.

As the IMDA has control over data protection and technological development, my policy can be implemented by the IMDA to regulate AI companies and medical institutions.

2.2.2 China

China has several foundational data protection laws[20], including the Cybersecurity Law, Data Security Law, and Personal Information Protection Law:

1. Cybersecurity Law emphasises that network operators must strictly protect the user information they collect and establish robust systems for user information protection.
2. Data Security Law requires that data processing activities comply with laws and regulations, respect public ethics and professional conduct, and fulfil obligations to protect data security.
3. Personal Information Protection Law stipulates that personal information processors must follow the principles of legality, legitimacy, necessity, and good faith.

In 2022, Administrative Measures for Cybersecurity in Medical and Health Institutions[21] further clarified the full-cycle responsibilities of medical institutions in data collection, storage, use, sharing, and destruction.

Additionally, local governments have issued more detailed implementation guidelines and regional policies tailored to their contexts. For example, according to a researcher in the area, some provinces have introduced regional health information platform data security management standards, specifying detailed requirements for data sharing and exchange.

2.2.3 United States

The U.S. adopts a multi-department regulatory model for managing medical data, involving:

1. Food and Drug Administration (FDA) evaluates the security and effectiveness of data related to medical devices.
2. Centers for Medicare & Medicaid Services (CMS) oversees the use of data related to coverage decisions under Medicare and Medicaid.
3. Department of Health and Human Services (HHS) is responsible for privacy protection, especially under the Health Insurance Portability and Accountability Act (HIPAA).

The FDA has proposed a regulatory framework for AI/ML-based software as a medical device[22]. However, this is simply a framework and could face challenges given the recent Big Beautiful Bill[12] that could prevent AI regulation.

Furthermore, the U.S. does not have a dedicated law specifically for medical data privacy. Instead, it relies on existing frameworks such as HIPAA, which applies to “covered entities” like hospitals and insurers, but offers limited regulation over non-clinical or consumer health data (e.g., fitness apps), leaving certain areas relatively underregulated. Given the fractured state of AI regulation, the following policy could instead be included in the HHS as an amendment to HIPAA to focus primarily on patient privacy.

2.2.4 European Union

The General Data Protection Regulation (GDPR), implemented in 2018, forms the core of the EU’s data privacy regime. Personal health data is classified as special category data, subject to stricter protections. The patient’s informed consent must be obtained, and the purpose of using health data must be clearly stated. The data minimisation principle must also be followed, where only necessary data should be collected and processed.

Additionally, the European Group on Ethics in Science and New Technologies (EGE) has published guidelines that 1) prohibit the misuse of sensitive data, 2) require algorithmic transparency from companies using medical data.
Specific to AI, the EU has implemented the AI Act (AIA)[23] in 2022 as one of the first pieces of legislation on AI use in the world. The AIA classifies AI into risk categories, where healthcare AI is classified under "high-risk AI" and subject to strict obligations. These include robust data governance, human oversight, traceability, and transparency of algorithms. The AIA complements the GDPR to ensure compliance with overall ethical and privacy standards.

However, differences in implementation across EU member states present challenges in consistent enforcement and policy execution at the national level. Some also argue that overly strict rules may hinder AI innovation, especially in healthcare startups and research institutions.

3. Key Stakeholders

This policy should apply to researchers and healthcare professionals developing AI healthcare models. It is recommended that the policy be implemented first in medical establishments such as hospitals, as they have on-the-ground access to patient data and hold greater responsibility in protecting patients. This can also simplify the excessive regulation needed to cover any individual involved in AI research on such data in the future. The policy should also be integrated alongside existing data protection laws in the country to minimise extra manpower required to uphold the policy.

3.1 Governments

Governments stand to benefit from this policy, which helps build public trust in emerging health technologies and allows national healthcare systems to reap the benefits of AI without centralising sensitive data. Countries can remain competitive in AI innovation and improve their citizens' quality of life.

However, governments are responsible for keeping pace with rapidly evolving AI and privacy technologies. Failure to do so could result in policy gaps or unaddressed system vulnerabilities. Enforcing compliance across hospitals, research institutions, and AI companies requires investment in oversight infrastructure, legal frameworks, and technical expertise that may be unevenly distributed across countries or jurisdictions. While the policy aligns with broader goals of data protection and digital innovation, its complexity and cost may pose challenges in implementation.

Governments can integrate this policy into existing healthcare privacy policies. As AI regulation is still developing, this policy is important to protect citizens. The policy can also be based on more foundational healthcare protection policies, which can improve its stability and adoption.

3.2 Hospitals

Each country has different healthcare systems, broadly split into public/non-profit hospitals and private/for-profit hospitals for this discussion. All hospitals will benefit from access to improved AI tools that support clinical decision-making while ensuring patient data is handled ethically and securely. With federated learning, data remains on-site, reducing the risk of breaches and misuse, and aligning with typically stronger public accountability requirements of these institutions.

Public hospitals may have greater access to public research institutions such as universities or government research institutions, which can encourage ease of integration for data into research. The framework also encourages closer partnerships with research institutions and AI developers, which could bring technical and financial resources into underfunded hospital systems. However, the technical and operational demands of implementing these measures, such as maintaining secure infrastructure, managing consent, and participating in secure aggregation protocols, could burden already resource-constrained public hospitals.

Private hospitals may see strategic advantages in adopting the proposed framework, particularly in maintaining patient trust and competitive positioning in a market increasingly concerned with data privacy. Private hospitals can access cutting-edge tools without sacrificing confidentiality or regulatory compliance by participating in collaborative AI development while retaining control over their patient data. However, implementing the technical components of federated learning requires financial investment and skilled personnel, which not all private institutions may have. Furthermore, compliance demands may reduce flexibility in pursuing external partnerships.

Still, research has shown that AI models matched the performance of human radiologists when acting as the second reader of mammography scans can streamline breast cancer diagnoses by cutting radiologists' workloads by at least 30%[25]. Given the evidence of early success of AI in healthcare decision-making, hospitals can improve patient care by making improved decisions using AI.

3.3 Research Institutions

Research institutions stand to gain immensely through their expanded access to real clinical data while minimising privacy concerns that could limit access under current regulations. Also, the emphasis on data security may ease the institutional review process.

However, the reduced access to raw data may impede more exploratory analysis. Researchers must also coordinate across multiple institutions, complicating the research process. For institutions without significant technical infrastructure, meeting the computational demands of privacy-preserving techniques may pose additional barriers to participation.

Still, data protection is necessary to ensure trust in research institutions such that individuals remain willing to provide their data in the future.

3.4 AI Companies

Similarly to research institutions, AI companies gain access to rich datasets and opportunities to build more robust, generalisable models through partnerships with hospitals and research institutions. The FL approach allows companies to develop healthcare solutions while adhering to strict privacy laws, enhancing their credibility and marketability in a highly regulated domain.

However, the framework also imposes significant limitations on direct data access, which may hinder model optimisation. Companies must also comply with technical and legal standards across multiple jurisdictions, which require extensive expertise and resources. For startups and smaller firms, these requirements may be a barrier to entry.

The framework actively encourages collaboration between companies and hospitals to pool resources together and share their expertise, mitigating some of the costs.

3.5 Patients

Patients are arguably the most protected under this policy, which strongly emphasises personal data privacy. Patients enjoy greater data privacy as FL ensures that sensitive health data remains within the institution where it was collected, substantially reducing the risk of data breaches or unauthorised access. Patients may benefit indirectly from AI models trained across multiple institutions, which can improve clinical decision-making. Research has shown outpatient diagnostic errors of 5.08%, or approximately 12 million US adults every year. About half of these errors could potentially be harmful. If AI can reduce even 5% of misdiagnoses, 0.6 million US adults can be protected every year[26].

However, there are some important costs to consider. Due to how AI models are trained, patients may have limited agency or visibility in how their data contributes to AI development, which may raise concerns about transparency. Some patients may be reluctant to allow their data to be used due to mistrust, reducing the volume and diversity of data available for model training. If the training data is not representative, resulting models may underperform for underrepresented populations, possibly worsening healthcare disparities.

With this framework, patients may trust AI models more, potentially becoming more willing to contribute to these models.

4. Timeline

The implementation plan will be as follows:

1. First, medical institutions should incorporate the proposed framework into their internal data protection policies. This may involve migrating patient data to secure cloud infrastructures to meet privacy requirements. To manage potential technical or financial challenges, hospitals can collaborate with national or regional health IT governance bodies for infrastructure support and funding.

2. Next, academic institutions, particularly those conducting AI medical research, should work with their ethics committees to introduce specific review protocols for AI-related data use. This may include assessments of model explainability, dataset bias, and patient consent practices. In tandem, universities may need to upgrade their computational infrastructure (e.g., expand GPU capacity or secure access to research clouds) to meet the technical demands of privacy-preserving large-scale AI model training.

3. In the longer term, governmental bodies should establish clear regulations governing collaborations between AI companies, medical institutions, and academic institutions. These regulations should include formalised data sharing contracts and mandatory audits. Rather than creating new legislation from scratch, these AI-specific rules could be incorporated as amendments to existing data protection laws, such as HIPAA (US) or the GDPR (EU), ensuring consistency with current legal frameworks.

5. Proposed Framework: Singapore

To improve existing policy, the following framework is designed for medical research involving AI. The framework focuses on ensuring that AI models are trained using medical data in a way that protects patient privacy and complies with existing legal regulations. The framework has a legal basis in Singapore, given better on-the-ground knowledge of research boundaries and legal practices.

Data Collection

- Individuals must provide informed consent before their data is used for research. This is currently already regulated in the PDPA. Their consent should include:
    - Clear descriptions of how their data will be used.
    - The purpose of AI training, including any risks and benefits.
    - The option to opt out at any time. However, as mentioned in Section 5.2.1, the opting-out process may not be easily achieved as the model has already converted training data into vector space, making it difficult to isolate individual data points.
- As IMDA often provides programmes and grants[27] for Singapore's technological development, some of its funding can be set aside for healthcare research. IMDA can run pilot programmes where the health data of deceased individuals is used to train AI models. Deceased individuals may provide a greater collection of data that includes more data points, which could improve model performance. However, this could create biased models, which is later addressed in the Model Evaluation section.

Data Security

- Basic security standards
    - Use advanced encryption (AES-256) for data storage and transmission. The PDPA currently regulates that an organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and the loss of any storage medium or device on which personal data is stored. While no specific actions are outlined in the Act, the IMDA can encourage secure encryption in its best practices section for organisations. All systems processing medical data for AI research should be hosted on secure platforms (e.g., HIPAA-compliant cloud infrastructure[24]). Systems processing medical data must comply with national standards outlined in the Cybersecurity Act 2018[23].
    - All data used in model training should be de-identified, where personal identifiers are replaced with unique pseudonyms, as is currently practised.
- Federated Learning security standards
    - The IMDA can encourage the adoption of FL to minimise data sharing. This can be included in the Emerging Technologies[28] IT Standards and Frameworks. Data can remain within local medical institutions. If local medical institutions are unable to train the model accurately, its data may be aggregated on a city or state level, up to where sufficient data is available for training. Central servers should only receive aggregated, noise-added updates, preventing reconstruction of any contributing data source.
    - On untrusted systems, homomorphic encryption techniques are recommended so that model updates are encrypted. This ensures no party can access the raw data or reverse-engineer the updates.

        - However, HE is known for its slow performance and computational requirements[29, 30], which some institutions may not have the capacity to handle. Hence, where homomorphic encryption is not feasible due to performance constraints, secure multiparty computation is recommended, based on early research of its relative success[31].
    - Differential privacy
        - Implement differential privacy during the model aggregation process to prevent the leakage of sensitive patient data through model updates. Differential privacy is found to be successful in preventing both gradient inversion (Section 4.2) and membership inference (Section 4.3) attacks.
    - Aggregation
        - Secure aggregation techniques, such as Bonawitz et al.'s protocol[32], should be used to ensure that model updates are combined so that no party can see or extract individual updates. Secure aggregation can reduce the effects of model poisoning (Section 4.1) and membership inference (Section 4.3)

Data Sharing

- Data Sharing Agreements (DSAs)
    - Formalise partnerships between hospitals, researchers, and AI companies with clear Data Sharing Agreements. Currently, IMDA provides a Data Sharing Framework[33] and samples. As it oversees AI companies, IMDA is at a prime spot for facilitating DSAs between AI companies, researchers, and hospitals. DSAs can include the following:
        - Explicitly outline data ownership, usage rights, and data protection responsibilities.
        - Specify which parties have access to the data and the conditions under which data may be shared or reused.
        - NDAs must be included to protect research results before publishing, and raw data
- Third-party data use
    - Any third-party AI companies or research institutions accessing the data must adhere to the same data protection standards with legally binding contracts that include penalties for violations. These contracts can be investigated by the PDPC for violations against personal data protection. The PDPA Offences and Penalties Section[34] can keep organisations in line. Specific penalties can be outlined in an amendment in the future.

Model Evaluation

- Model performance
    - Research on AI must ensure that the data used to train AI models represents diverse populations. In particular, this highlights how relying on data from deceased individuals to limit privacy risks could skew results due to age or sampling bias. Reasonable effort must be made to address these questions:
        - Effectiveness: Does the model improve patient outcomes?
        - Fairness: Is the model fair across different demographic groups (e.g., gender, race, socio-economic status)?
        - Privacy: Does the model ensure data protection and patient confidentiality?

    - The model must also be repeatedly tested on unseen data to verify that no malicious clients are involved in training, as discussed in mitigation techniques for model poisoning in Section 4.1. A malicious client is defined as an untrusted component that can collude in attacks during FL by affecting the global FL model's performance through participation in the training process.
- Model refinement
    - Continuous refinement based on feedback from healthcare workers, researchers, and patients is necessary to prevent model drift[35], where model performance degrades over time. This ensures that the models evolve to incorporate the latest clinical knowledge. There exists some work on correcting deployed models in a way that does not require re-training end-to-end (e.g. fine-tuning[36], and in-context learning[37, 38]). Still, more work remains, especially for AI systems with many interacting parts.

This framework extends current data protection legislation and ethical research standards. Hence, the IMDA can initially include this framework in its best practices. The PDPC could amend the PDPA to cover AI data protection further. As the IMDA regulates the overall technology sector, it can work closely with IT companies to encourage secure AI adoption. The government can regulate universities and hospitals (through the Ministry of Health) to integrate this framework into existing ethics boards to oversee research methodologies and data handling practices in healthcare research. Existing ethics boards should ensure that at least one individual with prior experience in AI is involved to understand technical details in data ingestion and model training. These boards will ensure that all partners (e.g., hospitals, researchers, AI companies) follow strict governance protocols for sharing and processing data. Much like how current boards operate, if the researchers do not outline sufficiently secure practices, their research will not be allowed to proceed. When submitting their research to journals, journals may not accept research that does not outline secure practices, although this may require further international coordination.

6. Future Updates

As AI models become more sophisticated, attacks will naturally increase in difficulty. To contend with more insidious attacks, it is necessary to consistently update the framework by working closely with researchers at the forefront of FL research, such as those in Singapore's national universities. Singapore's small size works to its advantage. The government can closely regulate institutions for its security and facilitate collaboration between various sectors.

7. References

1. Kaissis, G. A., Makowski, M. R., Rückert, D., & Braren, R. F. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. Nature Machine Intelligence, 2(6), 305–311. doi:10.1038/s42256-020-0186-1
2. McKinney, S. M., Sieniek, M., Godbole, V., Godwin, J., Antropova, N., Ashrafian, H., Back, T., Chesus, M., Corrado, G. S., Darzi, A., Etemadi, M., Garcia-Vicente, F., Gilbert, F. J., Halling-Brown, M., Hassabis, D., Jansen, S., Karthikesalingam, A., Kelly, C. J., King, D., Ledsam, J. R., … Shetty, S. (2020). International evaluation of an AI system for breast cancer screening. *Nature*, *577*(7788), 89–94. https://doi.org/10.1038/s41586-019-1799-6
3. Ardila, D., Kiraly, A. P., Bharadwaj, S., Choi, B., Reicher, J. J., Peng, L., Tse, D., Etemadi, M., Ye, W., Corrado, G., Naidich, D. P., & Shetty, S. (2019). End-to-end lung cancer screening with

three-dimensional deep learning on low-dose chest computed tomography. *Nature medicine*, *25*(6), 954–961. https://doi.org/10.1038/s41591-019-0447-x

4. Pinker, K., Chin, J., Melsaether, A. N., Morris, E. A. & Moy, L. Precision medicine and radiogenomics in breast cancer: new approaches toward diagnosis and treatment. Radiology 287, 732–747 (2018).
5. Lu, H. et al. A mathematical-descriptor of tumor-mesoscopic-structure from computed-tomography images annotates prognostic- and molecularphenotypes of epithelial ovarian cancer. Nat. Commun. 10, 764 (2019).
6. Kaissis, G. et al. A machine learning model for the prediction of survival and tumor subtype in pancreatic ductal adenocarcinoma from preoperative difusion-weighted imaging. Eur. Radiol. Exp. 3, 41–41 (2019).
7. Cui, E. et al. Predicting the ISUP grade of clear cell renal cell carcinoma with multiparametric MR and multiphase CT radiomics. Eur. Radiol. 30, 2912–2921 (2020).
8. Rajpurkar, P. et al. CheXNet: radiologist-level pneumonia detection on chest X-rays with deep learning. Preprint at https://arxiv.org/ abs/1711.05225 (2017).
9. Florian Bourse et al. Fast Homomorphic Evaluation of Deep Discretized Neural Networks. In Advances in Cryptology, 2018.
10. Pejic, I., Wang, R., & Liang, K. (2022). Effect of homomorphic encryption on the performance of training federated learning generative adversarial networks. arXiv preprint arXiv:2207.00263.
11. Ehsan Hesamifard et al. Deep neural networks classification over encrypted data. In ACM Conference on Data and Application Security and Privacy, 2019.
12. H.R.1 - One Big Beautiful Bill Act 119th Congress (2025-2026), Sec 0012
13. De Cristofaro, E. (2020). An overview of privacy in machine learning. arXiv preprint arXiv:2005.08679.
14. Melanie Sloan, Michael Bosley, Caroline Gordon, Thomas A Pollak, Farhana Mann, Efthalia Massou, Stephen Morris, Lynn Holloway, Rupert Harwood, Kate Middleton, Wendy Diment, James Brimicombe, Elliott Lever, Lucy Calderwood, Ellie Dalby, Elaine Dunbar, David D'Cruz, Felix Naughton, 'I still can't forget those words': mixed methods study of the persisting impact on patients reporting psychosomatic and psychiatric misdiagnoses , Rheumatology, Volume 64, Issue 6, June 2025, Pages 3842–3853, https://doi.org/10.1093/rheumatology/keaf115
15. Rodriguez, A., Tuck, C., Dozier, M. F., Lewis, S. C., Eldridge, S., Jackson, T., Murray, A., & Weir, C. J. (2022). Current recommendations/practices for anonymising data from clinical trials in order to make it available for sharing: A scoping review. Clinical trials (London, England), 19(4), 452–463. https://doi.org/10.1177/17407745221087469
16. Gadotti, A., Rocher, L., Houssiau, F., Crețu, A.M., De Montjoye, Y.A.: Anonymization: The imperfect science of using data while preserving privacy. Science Advances 10(29), eadn7053 (2024)
17. Olatunji, I. E., Rauch, J., Katzensteiner, M., & Khosla, M. (2024). A review of anonymization for healthcare data. Big data, 12(6), 538-555.
18. Tabiri Aning, Edmond and Agnihotri, Nishant, Data Security: A Study of Data Anonymization And Several Techniques (March 13, 2024). Available at SSRN: https://ssrn.com/abstract=4757543 or http://dx.doi.org/10.2139/ssrn.4757543
19. Personal Data Protection Act 2012 - Singapore Statutes Online. (n.d.). Singapore Statutes Online. Retrieved July 24, 2025, from https://sso.agc.gov.sg/Act/PDPA2012
20. Article 1226 of the Civil Code of the People's Republic of China
21. National Health Commission. Notice on Issuing the Measures for the Administration of Cybersecurity in Medical and Health Institutions [EB/OL]. http://www.nhc.gov.cn/guihuaxxs/s10743/202208/50e2ef41b7554ae894053bcac32b79f0.shtml, 2022-8-8.
22. Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD), FDA, 2025
23. Cybersecurity Act 2018 - Singapore Statutes Online. (n.d.). Singapore Statutes Online. Retrieved July 24, 2025, from https://sso.agc.gov.sg/Acts-Supp/9-2018/

24. (OCR), O. for C.R. (2023) Cloud computing, HHS.gov. Available at: https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html (Accessed: 21 July 2025).
25. Sharma N et al. Retrospective large-scale evaluation of an AI system as an independent reader for double reading in breast cancer screening. doi: 10.1101/2021.02.26.21252537.
26. Benaissa, A., Retiat, B., Cebere, B., & Belfedhal, A. E. (2021). Tenseal: A library for encrypted tensor operations using homomorphic encryption. *arXiv preprint arXiv:2104.03152*.
27. How We Can Help. (2024, July 11). IMDA. Retrieved July 24, 2025, from https://www.imda.gov.sg/how-we-can-help?
28. IMDA. (n.d.). Emerging Technologies. IT Standards and Frameworks. https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/it-standards-and-frameworks/emerging-technologies
29. C. Gentry and S. Halevi, "Implementing gentry's fully-homomorphic encryption scheme," in Annual international conference on the theory and applications of cryptographic techniques. Springer, 2011, pp. 129– 148.
30. J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in Advances in Cryptology– ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I 23. Springer, 2017, pp. 409– 437.
31. Secure Multiparty generative AI. (n.d.). https://arxiv.org/html/2409.19120v1
32. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Seth, K. (2016). Practical secure aggregation for federated learning on user-held data. arXiv preprint arXiv:1611.04482.
33. IMDA. (n.d.). About the Trusted Data Sharing Framework. IMDA. Retrieved July 24, 2025, from https://www.imda.gov.sg/how-we-can-help/data-innovation/trusted-data-sharing-framework
34. Personal Data Protection Act 2012 - Singapore Statutes Online. (n.d.). Singapore Statutes Online. Retrieved July 24, 2025, from https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P110-#pr51-
35. Bayram, F., Ahmed, B. S., & Kassler, A. (2022). From concept drift to model degradation: An overview on performance-aware drift detectors. Knowledge-Based Systems, 245, 108632.
36. E. J. Hu, P. Wallis, Z. Allen-Zhu, Y. Li, S. Wang, L. Wang, W. Chen, et al. Lora: Low-rank adaptation of large language models. In International Conference on Learning Representations, 2022.
37. J. Wei, X. Wang, D. Schuurmans, M. Bosma, F. Xia, E. H. Chi, Q. V. Le, D. Zhou, et al. Chain-of-thought prompting elicits reasoning in large language models. In Advances in Neural Information Processing Systems, 2022.
38. S. Chan, A. Santoro, A. Lampinen, J. Wang, A. Singh, P. Richemond, J. McClelland, and F. Hill. Data distributional properties drive emergent in-context learning in transformers. Advances in Neural Information Processing Systems, 35:18878–18891, 2022.