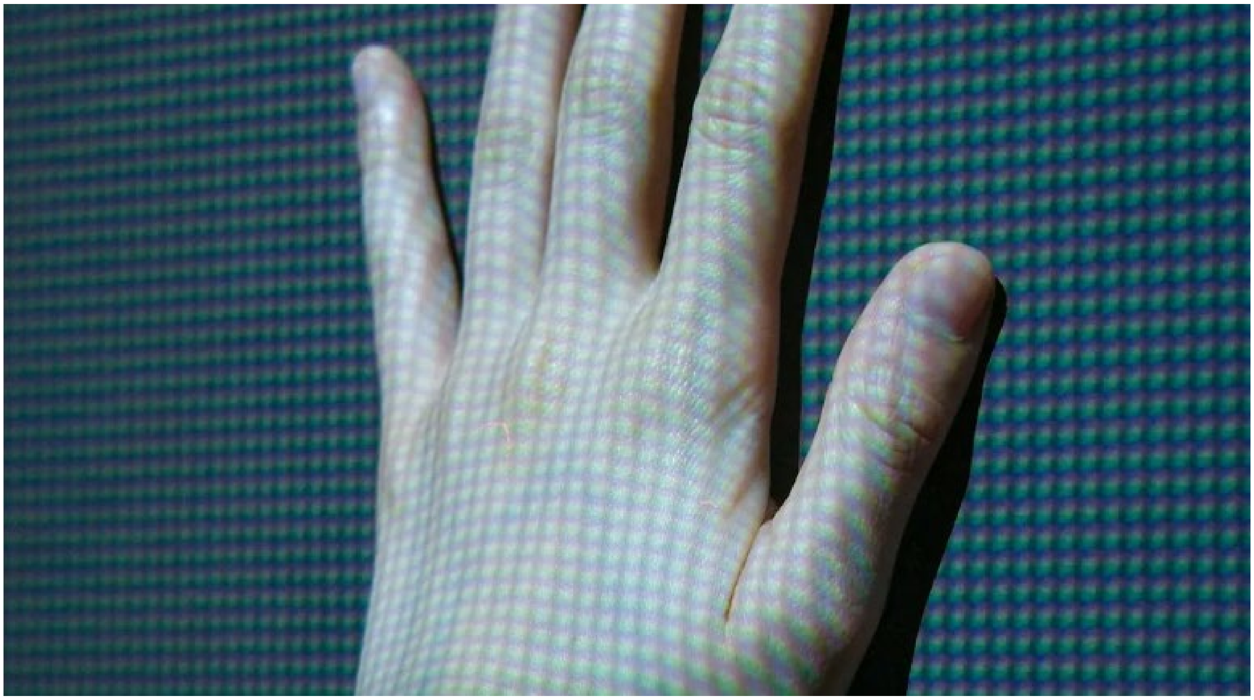
Health Data and Biometrics in AI: Regulatory Risks for Hong Kong Enterprises

AI boosts innovation for Hong Kong businesses but demands careful handling of health and biometric data to ensure privacy and compliance.



The adoption of artificial intelligence (AI) is transforming the business landscape, enabling enterprises across finance, healthcare, retail, and technology to enhance operational efficiency and deliver tailored services. Processing sensitive personal data, such as health records and biometric identifiers, offers significant opportunities for innovation. Yet, these technological advancements also raise concerns about privacy and data security. These advancements are subject to stringent oversight under Hong Kong's Personal Data (Privacy) Ordinance (Cap.486) (PDPO). Non-compliance with the PDPO may result in financial penalties, legal liabilities, and reputational damage. The Office of the Privacy Commissioner for Personal Data (PCPD) issued the Artificial Intelligence: Model Personal Data Protection Framework (AI Framework) in 2024 to guide organizations in managing privacy risks associated with AI. Understanding the PDPO, the AI Framework, regulatory risks of processing sensitive data, compliance strategies, and the evolving regulatory landscape is crucial for business operators in Hong Kong.

The PDPO

The PDPO governs the collection, processing, and use of personal data, defined as data relating directly or indirectly to a living individual, from which it may be practicable for the identity of the individual to be directly or indirectly ascertained, and in a form in which access to or processing of the data is practicable. This includes sensitive health records (e.g., medical diagnoses, genetic profiles) and biometric identifiers (e.g., facial recognition, fingerprints). Applicable to all organizations operating within Hong Kong's jurisdiction, it is administered by the PCPD and structured around 6 Data Protection Principles (DPPs):

- DPP 1. Purpose and Collection: Personal data must be collected for a lawful purpose directly related to the organization's functions.
- DPP 2. Accuracy and Retention: Data must be accurate, up-to-date, and not excessive for its intended purpose.
- DPP 3. Use: Data must only be used for the purpose for which it was collected, unless further consent is obtained.

- DPP 4. Security: Reasonable measures must be implemented to protect data from unauthorized access, loss, or misuse.
- DPP 5. Information: Individuals must be informed about data use through a Personal Information Collection Statement (PICS).
- DPP 6. Access and Correction: Individuals have the right to access and correct their personal data.

Non-compliance may lead to enforcement notices from the PCPD, with failure to comply constituting a criminal offense punishable by fines up to HK$50,000, a daily penalty of HK$1,000, and imprisonment for up to two years. Mishandling sensitive data may also result in reputational harm and civil claims. Subsequent convictions can result in a maximum fine of HK$100,000 and imprisonment for 2 years, with a daily penalty of HK$2,000.

The AI Framework published by PCPD

On June 11, 2024, the PCPD released the AI Framework to address privacy risks in AI systems processing personal data, particularly health records and biometric identifiers. Extending the 2021 Guidance on the Ethical Development and Use of AI, this non-binding framework targets organizations using AI systems, offering structured guidance for PDPO compliance and ethical AI use. It includes 4 key areas:

1. AI Strategy and Governance: Establish an AI strategy with senior management support, conduct due diligence on AI suppliers for PDPO compliance, form a cross-disciplinary AI governance committee, and train employees on data privacy and ethics.
2. Risk Assessment and Human Oversight: Conduct risk assessments to evaluate privacy, legal, and ethical impacts, with documented mitigation plans. Human oversight is required to validate AI decisions.
3. AI Customization and Management: Minimize personal data use, test systems for security and fairness, and maintain an AI Incident Response Plan for breach resolution.
4. Stakeholder Engagement: Disclose AI usage transparently, explain decision-making processes, and provide mechanisms for individuals to access or correct data, aligning with DPP5.

Regulatory Risks

The use of AI to process health records and biometric identifiers presents significant regulatory risks for businesses in Hong Kong. Insurance companies, for instance, may collect biometric data, such as genetic profiles or health metrics, for risk assessment or wellness programs, subject to strict PDPO compliance. Data breaches pose a major threat, as these data types are prime targets for cyberattacks. Unauthorized access to a healthcare provider's AI system or a retailer's facial recognition tool could lead to financial penalties, enforcement actions, and diminished customer trust. Processing health data for unauthorized purposes, such as marketing without consent, violates DPP3 and may trigger regulatory sanctions. Failure to transparently disclose AI-driven data practices contravenes DPP5, risking customer confidence. Algorithmic bias from flawed training data may produce discriminatory outcomes, such as biased credit assessments or hiring decisions, exposing organizations to legal and ethical challenges. Overreliance on automated decision-making without human oversight may infringe individuals' rights under DPP6 to contest AI-generated outcomes.

Compliance Strategies

To mitigate these risks, organizations should adopt robust measures aligned with the PDPO and the AI Framework. Conducting Privacy Impact Assessments (PIAs) before deploying AI systems enables identification and mitigation of privacy risks, particularly for sensitive data. For example, a retailer implementing AI-driven facial recognition should use a PIA to assess data exposure risks and implement safeguards. Data minimization, consistent with DPP2, involves collecting only essential data and anonymizing it to limit breach exposure. Human oversight ensures AI decisions are reviewed for fairness and accuracy, such as validating AI diagnostics in healthcare settings. Security measures, including encryption and regular audits, are critical to protect data from cyber threats. Transparent communication through clear PICS informs individuals about AI data practices, ensuring DPP5 compliance. Employee training on PDPO obligations and the AI Framework's ethical guidelines fosters responsible data handling.

The Evolving Regulatory Landscape

Hong Kong's regulatory framework is evolving to address AI and sensitive data processing challenges. In the future, industries such as finance and healthcare may develop specific guidelines, and companies will need to develop corresponding compliance plans. Global standards, such as the European Union's General Data Protection Regulation, emphasize stringent data protection and accountability, aligning with Hong Kong's regulatory direction. Businesses should strengthen data governance and breach response protocols to meet these requirements.

Conclusion

The use of AI to process sensitive health and biometric data offers significant opportunities for Hong Kong businesses but requires strict adherence to the PDPO and adoption of the AI Framework. Risks such as data breaches, unauthorized data use, algorithmic bias, and lack of transparency may lead to financial penalties, legal liabilities, and reputational harm. By implementing Privacy Impact Assessments, data minimization, human oversight, robust security, transparent communication, and employee training, organizations can mitigate these risks and responsibly leverage AI. As Hong Kong's regulatory landscape evolves, with potential PDPO amendments and further AI guidelines expected, enterprises must remain proactive to ensure compliance while remaining competitive.

To explore how JML can assist your enterprise in navigating the complex legal landscape of AI-driven data processing and ensuring compliance with Hong Kong's PDPO and AI Framework, please scan the QR code below to discover our legal services.

Information in this article is for general reference only and should not be relied on as legal advice.