Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 4 >>> APRIL 2016

Hong Kong

Sharing is Caring: New Electronic Health Record Sharing System for Hong Kong

By Gabriela Kennedy and Karen H. F. Lee

The ability for doctors, dentists and pharmacists to have quick and ready online access to an individual's medical profile and history (e.g. list of allergies, history of illnesses which may show a pattern indicating a more serious ailment, etc), is a normal expectation in the digital age. Technology nowadays supports the delivery of quality medical services. However, as is always the case with technology, convenience and efficiency must be balanced against the protection of personal data and privacy. As health records contain particularly sensitive information, should they require a higher degree of protection than that afforded to other personal data?

Gabriela Kennedy is a partner at Mayer Brown JSM, Hong Kong.

Karen H. F. Lee is a senior associate at Mayer Brown JSM, Hong Kong

On 2 Dec. 2015, after years of consultation and debate, Electronic Health Record Sharing System Ordinance (Cap. 625) (EHRSSO) came into effect in Hong Kong. The EHRSSO allows health-care professionals and public and private hospitals to collect, share and store patients' electronic health records via the Electronic Health Record Sharing System (eHR System). Patients and health-care providers can join the eHR System on a voluntary basis. The eHR System brings about a major change for private health-care providers in Hong Kong, most of them operating in small practices and still having paper files and records. The public sector, by contrast, operates under the Hospital Authority and the Department of Health, which has had in place a well developed electronic data management system for a good few years now, and boasts one of the largest in-

formation technology workforces in town. The discrepancy between the IT systems for public health-care versus private health-care is huge, and investment of time and money will be required from the private health sector to automate their systems in order to be able to register under the EHRSSO.

Health Records = Sensitive Data?

The medical data of an individual generally falls within the scope of "personal data" or "personal information" (i.e. data from which it is practicable to identify an individual), and is protected under applicable data privacy laws. This is the case in many jurisdictions in the Asia-Pacific region.

Some jurisdictions provide a higher threshold of protection for "sensitive data" or "sensitive information," which usually include health records. Australia and Malaysia generally prohibit the collection and use of sensitive information, unless the relevant individual has given his/her explicit consent or one of the exemptions under the legislation apply (for example, where the collection is sanctioned by a court order).

The Electronic Health Record Sharing System Ordinance allows health-care professionals and public and private hospitals to collect, share and store patients' electronic health records via the Electronic Health Record Sharing System.

Australia has specific provisions that regulate the handling of health information in its data privacy legislation. Under the Australian Privacy Act 1988 (as amended up to Act No. 157, 2015) (Australian Privacy Act), "health information" is defined to include "information or an opinion" about "the health, including an illness, disability or injury (at any time), of an individual," "an individual's expressed wishes about the future provisions of health services to the individual," or "a health service provided, or to be provided, to an individual," to the extent that it is also personal information. The Australian Privacy Act specifically allows health information to be collected by an organisation, if it is necessary in order to provide a health service to the individual and the collection is either required or authorised under Australian law.

In contrast, Hong Kong and Singapore data privacy laws don't distinguish between personal data versus sensitive data, nor do they impose more stringent restrictions on the use of sensitive data, over and above the protections applied to personal data in general.

Despite there being no separate category of "sensitive data" under the Hong Kong Personal Data (Privacy) Ordinance (PDPO), the Hong Kong Privacy Commissioner (PC) tends to take a stricter approach on the application of the Data Protection Principles (DPPs) under the PDPO in respect of personal data that is perceived as being particularly "sensitive," taking into account the nature of the information (e.g. health records, biometric data and Hong Kong identity card numbers) and the context in which it is collected and used.

During the consultation period for the Personal Data (Privacy) (Amendment) Ordinance 2012 (which introduced changes to the PDPO), the Hong Kong Government considered introducing a new category of "sensitive data," which would have been subject to more rigorous controls. However, this proposal wasn't pursued due to a lack of consensus on the coverage, regulatory model and sanctions for the protection of sensitive data.[1] While the proposal to introduce a new regime to protect "sensitive data" was set aside, the Government asked the PC to issue codes and guidelines of best practices on the handling and use of personal data, including health records.[2]

Electronic Health Record Sharing System Ordinance

The EHRSSO provides the legal framework for the collection, sharing, use and safeguarding of health records via the eHR System by health-care providers.

The eHR System has the potential to become an efficient platform for both private and public health-care providers to share and access patient records. On 13 March 2016, the platform went live, and patients and health-care providers can now join the eHR System on a voluntary basis. A newly appointed Commissioner for the Electronic Health Record (eHR Commissioner) will oversee the operation and regulation of the eHR System in accordance with the EHRSSO.

Hong Kong isn't the first Asia Pacific country to launch an electronic health record system. In July 2012, Australia launched its national health record system under the Australian My Health Care Records Act (as amended in November 2015 and formerly known as the Personally Controlled Electronic Health Records Act 2012) (Australian Health Records Act). Similar to the EHRSSO, the Australian Health Records Act introduced a legislative framework, which allows patients' health records to be shared amongst health-care providers (unless the pa-

[1] The Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance issued in October 2010 by the Hong Kong Government.

[2] *Id.* 2.

   ISSN 1473-3579

tient hasn't provided her consent or has withdrawn it). The Australian Government is currently running trials in the Nepean Blue Mountains in New South Wales and Northern Queensland. All individuals located in these areas will automatically have a My Health Record created for them, unless they inform the relevant regulator that they wish to opt out. If the trials result in a high adoption rate of the My Health Record system, then the Australian Government may consider switching to a national opt-out scheme from its current opt-in scheme.

In June 2011, Singapore launched its National Electronic Health Record system. All Singapore residents are automatically included in the system, unless they have opted-out. In contrast, Hong Kong has preferred an opt-in system, as individuals must take steps to register and join the eHR System. At the end of 2015, Singapore launched a new online portal and an application (known as HealthHub), which allows Singaporean nationals and permanent residents to access their public health records online. Some of the information available is derived from the National Electronic Health Record.

Hong Kong has preferred an opt-in system, as individuals must take steps to register and join the Electronic Health Record Sharing System.

Sharing Health Records—Does It Hurt?

Under the EHRSSO, individuals who register with the eHR System are required to provide two separate consents—their consent to join and participate in the eHR System, and a separate consent to allow the sharing of all their health records with specific health-care providers (Sharing Consent).[3] Only health-care providers to whom an individual has provided their Sharing Consent will be able to access the individual's electronic health record.

Even after an individual's Sharing Consent has been obtained, health-care providers are still obligated to ensure that access to any health records on the eHR System is only allowed on a need-to-know basis. Health-care providers must take reasonable steps to ensure that only their relevant staff (i.e. doctors, pharmacists, etc) can access the parts of the health record stored on the eHR System, which are solely needed in order for them to provide the relevant health-care service to the patient.[4] This will require a lot of discernment on the part of medical staff, and clean categorisation and separation of data. The opportunity for access to more data than needed remains.

The above provisions were agreed by the Legislative Council and were generally non-contentious. During the consultation period for the introduction of the EHRSSO, an area of much debate surrounded the issue of whether or not an individual could restrict the scope within which her data is shared. While the efficient access to electronic health data is the main purpose and benefit of having an eHR System, patients have a reasonable expectation of (data) privacy, and therefore should be entitled to control exactly what data is being shared and with whom.

Given this, it was proposed that instead of individuals only being able to provide an "all or nothing" consent (i.e. consenting to specific health-care providers accessing all of their medical records pursuant to the Sharing Consent), they should also be allowed to specify certain types of data that would require their further separate consent before such data could be accessed (i.e. a "safe deposit box" of information). The downside of allowing individuals to pick and choose what data they shared, is that this might undermine the very objective of the eHR System and render it inoperable.

Patients can withdraw their consent at any time, and health-care providers must explain the impact of the patient's withdrawal of consent

In the end, due to the sensitive nature of health data, the Government decided to strike a balance between protecting patients' privacy and the overall intent of the eHR System, which is to enable the sharing of such data amongst health-care providers. In addition to a provision requiring each patient to provide their general Sharing Consent,[5] provisions were also introduced that allow an individual to submit a request to restrict the scope of sharing of specific health data[6] (Specific Consent). The scope of such Specific Consent is to be specified at a later date by the eHR Commissioner. The provisions regarding the Specific Consent aren't yet in operation, and are only intended to take effect after a further study and consultation is carried out on how they should be implemented.

eHR System and the PDPO

The EHRSSO and PDPO are intended to be in synch and to achieve the protection of the privacy and security of patients' personal data collected and stored on the eHR System. This means that there will likely be crossover between the handling of privacy issues between the eHR Commissioner and the PC. For the purposes of the PDPO, both the eHR Commissioner and health-care providers are considered data users in relation to individuals' health data.

In February 2016, the PC issued two Information Leaflets on the EHRSSO. One was aimed at providing advice to health-care providers on compliance with the PDPO when using or sharing medical data via the eHR Sys-

[3] Section 12 of the EHRSSO. Note that a Sharing Consent is deemed to be given to the Department of Health and the Hospital Authority when the patient registers and gives his consent to join the eHR System (Section 16 of EHRSSO).

[4] Section 37(2) of the EHRSSO.

[5] Section 12 of the EHRSSO.

[6] Section 17 and 18 of EHRSSO.

tem[7] (Healthcare Providers Information Leaflet), and the second was aimed at providing practical advice to individuals who are interested in registering with the eHR System.[8] The PC specifically refers to health records as "sensitive personal data" in the Healthcare Providers Information Leaflet, even though the PDPO doesn't expressly recognise a separate category of sensitive data.

In brief, the Healthcare Providers Information Leaflet advises that:

(a) the eHR System is voluntary, and patients must give two consents: (i) to join the eHR System; and (ii) a separate consent to allow their health records to be shared with specific health-care providers;

(b) patients can withdraw their consent at any time, and health-care providers must explain the impact of the patient's withdrawal of consent on the heath-care services that they may receive, and how such withdrawal of consent can be made to the eHR Commissioner;

(c) health-care providers must explain the operation of the eHR System in detail to patients, to ensure they understand the implications on their personal data privacy by sharing their health records;

(d) health-care providers must ensure that their health-care professionals only have access to the health records on a need-to-know basis (e.g. setting access restrictions, implementing internal codes dealing with the confidentiality of the health records, etc);

(e) health-care professionals should exercise their professional judgment to only access the medical data that is necessary in order to provide the relevant health-care service;

(f) health-care providers should ensure that the health records are accurate, and only personal data that is necessary and beneficial for the continuity of health-care should be retained on the eHR System;

(g) health-care providers must implement reasonable practicable steps to protect personal data retained on the eHR System;

(h) any data breaches should be promptly notified to the eHR Commissioner and the PC;

(i) use of the personal data contained in the eHR System for direct marketing purposes is a criminal offence, but health-care providers can still use the personal data stored on their local system for direct marketing, so long as they comply with the PDPO requirements;

(j) health-care providers should amend their personal data privacy policies to take into account the uploading of patients' personal data onto the eHR System; and

(k) if the health-care provider receives any data access request from a patient in respect of personal data uploaded onto the eHR System by another health-care provider, then they must inform the patient that their data access request should be referred to the eHR Commissioner.

Offences Under the EHRSSO

In order to give the EHRSSO more "teeth," and to reflect the seriousness of the potential misuse of health records or of any unauthorised access to the eHR System, the government introduced new offences in the EHRSSO[9] .

Under the EHRSSO, a person commits an offence if:

(a) she knowingly impairs the operation of the eHR System;

(b) she knowingly causes a computer to perform a function so as to obtain unauthorised access to data contained in an electronic health record;

(c) she knowingly damages data contained in an electronic health record (without lawful excuse);

(d) she knowingly causes access or modification to data contained in an electronic health record, or causes the accessibility, reliability, security or processing of such data to be impaired;

(e) she uses or transfers another person's data contained in an electronic health record for direct marketing purposes;

(f) with the intent to evade a data access or correction request, she alters, falsifies, conceals or destroys any data contained in an electronic health record; or

(g) she makes a false statement for the purposes of enabling a patient to provide his/her consent to the sharing of their data.

Most of the above offences can incur a fine of up to HK$ 100,000 ($12,890) and/or maximum imprisonment of up to 2 or 5 years, save for a breach of the direct marketing prohibition which can result in a maximum fine of up to HK$ 1,000,000 ($128,906) and 5 years imprisonment (which mirrors the penalty for a direct marketing offence under the PDPO).

The offences under the EHRSSO are broader then the related computer crime offences under the Crimes Ordinance (Cap. 200) (CO), or the direct marketing offences under the PDPO. However, the same acts that give rise to one of the above offences, could also amount to a breach of the PDPO or a crime under the CO, and may come under dual scrutiny of both the PC and eHR Commissioner. If any complaint is issued relating to a breach of the EHRSSO and/or PDPO, then the PC and eHR Commissioner both have the power to refer the complaint to the police for criminal investigation. The police can then determine, based on the facts of each case, whether or not it is more appropriate to charge the

[7] Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Health-care Providers and Health-care Professionals).

[8] Electronic Health Record Sharing System and Your Personal Data Privacy (10 Privacy Protection Tips).

[9] Sections 42 to 47 of the EHRSSO.

   ISSN 1473-3579

offender for a crime under the EHRSSO, the PDPO or the CO, or under all of them. In general, the more specific offence applicable to the facts of the case will be invoked and charged by the Police against the offender.

Under Section 161 of the CO, it is an offence to obtain access to a computer in order to commit an offence or with dishonest intent to deceive or cause loss, or to make a dishonest gain. While the Government decided to create a more specific computer related offence under the EHRSSO directly in relation to the eHR System, i.e. causing a computer to perform a function in order to obtain unauthorised access to data contained in the eHR System, restricting the scope of the offences to the use of a computer may be limiting, as many other devices, such as a smart phone or tablet, could be used to access the eHR System. Indeed, this is already the case in Singapore where electronic health records can be accessed through the HealthHub app, and health-related apps linking patients to health-care providers in a more de-centralised system are being launched in China.

Under the Electronic Health Record Sharing System Ordinance, extreme caution needs to be exercised by health-care providers if they decide to disclose patients' personal data to third parties.

To allow for future technological developments, further offences were introduced under the EHRSSO, not specifically limited to any means or methods of committing the offence. It is an offence under the EHRSSO to cause any damage or to obtain unauthorised access to the data on the eHR System, or to cause impairment of the accessibility, reliability, security or processing of such data or the operation of the eHR System.

Many health-care practitioners monetise patients' data by providing it to third parties for medical research or for direct marketing. Under the EHRSSO, extreme caution needs to be exercised by health-care providers if they decide to disclose patients' personal data to third parties. Whilst the direct marketing offences under the PDPO will only arise if the data user fails to provide the data subject with the required notice and to obtain the data subject's consent, no such procedure applies under the EHRSSO. The EHRSSO makes it an absolute offence for the eHR Commissioner, any health-care provider or any health-care professional to use or transfer any of the data contained on the eHR System for direct marketing (even if an individual's consent has been obtained). Unlike the PDPO, this absolute prohibition isn't expressly limited to "personal data," but applies to any data or information of a person contained in the electronic health record. This was reemphasised by the PC in the Healthcare Providers Information Leaflet, thus clarifying that the stricter offence under the EHRSSO would essentially take precedence over the direct marketing provisions under the PDPO.

If health-care providers have personal data stored on their own local system, the PC has stated that they can still use such personal data for direct marketing purposes, subject to their compliance with the PDPO requirements. However, in practice, it may be difficult for a health-care provider to prove that it utilised the patient's personal data stored on its own local system, rather than their electronic health records on the eHR System.

Conclusion

Electronic health records will make the sharing of information easier, and can assist not only with providing better and more efficient medical services to patients, but also assist with medical research and monitoring potential pandemics. Yet greater access, comes with greater vulnerabilities. Cybersecurity and data hacks make headlines almost on a daily basis, and individuals are more aware and concerned than ever before about their data privacy rights and the security of their data.

The offences introduced by the EHRSSO may act as a deterrent against any misuse of health records or the eHR System, but the EHRSSO provides no specific legal obligation concerning the security measures or safeguards that need to be implemented to prevent cyberhacks. The eHR Commissioner and health-care providers would still, however, need to comply with the Codes of Practice issued by the eHR Commissioner and the general data security obligation under the PDPO, i.e. to take reasonably practicable steps to ensure the security of personal data and to protect it against any unauthorised or accidental access, processing, erasure, loss or use.

The Codes of Practices that have so far been issued by the eHR Commissioner include a Code of Practice for Healthcare Professionals and Code of Practice for Management Executives, Administrative and Technical Staff using eHRSS[10], which contain obligations on health-care providers to implement specific security measures (e.g. maintain security in wireless networks for computers connecting to the eHR System, install appropriate anti-virus software, record and manage access rights, etc). These Codes aren't mandatory, but the eHR Commissioner has the power to cancel a health-care provider's registration with the eHR System if they are found to be in breach of any of the Codes of Practice[11]. We expect further amendments or additional codes and guidelines to be issued by the eHR Commissioner and PC on the exact security measures (including IT safeguards) to be adopted.

[10] These Codes collectively form the Code of Practice for Using eHR for Healthcare.

[11] Section 25(1)(a)(ii) of the EHRSSO.