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?

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...
Health Records = Sensitive Data?

The Australian Health Records Act introduced a legislative framework, which allows patients' health records to be shared amongst health-care providers (unless the patient objects). The Act specifically allows health-care professionals and health-care providers to share and access patient records. On 13 November 2015 and formerly known as the Personally Controlled Electronic Health Records Act 2012), the Australian My Health Care Records Act (as amended in Act No. 157, 2015) (Australian Privacy Act). Patients have the right to view, amend, and share their personal health records.

During the consultation period for the Personal Data Protection (Amendment) Ordinance 2012 (which were closed changes to the PDPO), the Hong Kong Government considered introducing a new subject of “sensitive data,” which would have been subject to more rigorous controls. However, the provision was dropped due to a lack of consensus on the coverage, regulatory model and sanctions for the protection of sensitive data. While the proposed introduction was aimed to protect “sensitive data,” there are already quite comprehensive frameworks available in the first Asia Pacific country to launch its national health record system under the Australian My Health Care Records Act (as amended in 2012) (Australian Privacy Act). Patients have the right to view, amend, and share their personal health records.

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, nor do they impose more stringent restrictions on the use of sensitive data. 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.

The EHRSSO provides the legal framework for the collection, sharing, use and safeguarding of health records. The EHRSSO allows health-care professionals and health-care providers to share and access patient records. On 13 November 2015 and formerly known as the Personally Controlled Electronic Health Records Act 2012), the Australian My Health Care Records Act (as amended in Act No. 157, 2015) (Australian Privacy Act). Patients have the right to view, amend, and share their personal health records.

The PDPO in respect of personal data that is perceived as being particularly “sensitive,” taking into account the nature of the information (e.g. medical 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 Protection (Amendment) Ordinance 2012 (which were closed changes to the PDPO), the Hong Kong Government considered introducing a new subject of “sensitive data,” which would have been subject to more rigorous controls. However, the provision was dropped due to a lack of consensus on the coverage, regulatory model and sanctions for the protection of sensitive data.

While the proposed introduction was aimed to protect “sensitive data,” there are already quite comprehensive frameworks available in the Asia Pacific region.

Some jurisdictions provide a higher threshold of protection for “sensitive data” or “sensitive information,” 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.

Australia has specific provisions that regulate the handling of health information in its data privacy legislation. Under the Australian Privacy Act (as amended up to Act No. 437, 2011) (Australian Privacy Act), “health information” is defined to include “information or an opinion about a health service provided, or to be provided, to an individual concerning the health of an individual... or an individual’s expressed wishes about the future provision of health services to the individual... or an individual’s expressed wishes about the future provision of health services to the individual, or a health service provided, or to be provided, to an individual concerning the health of an individual.” The Australian Privacy Act specifically allows health information to be used for the purposes of the health service provided, or to be provided, to the individual, or for the administration of the health service to the individual. The Australian Privacy Act also provides for the protection of health information, unless the relevant individual has given his/her explicit consent or one of the exemptions under the act.

Health Records = Sensitive Data?

The Australian Privacy Act specifically allows health information to be used for the purposes of the health service provided, or to be provided, to the individual, or for the administration of the health service to the individual. The Australian Privacy Act also provides for the protection of health information, unless the relevant individual has given his/her explicit consent or one of the exemptions under the act.

During the consultation period for the Personal Data Protection (Amendment) Ordinance 2012 (which were closed changes to the PDPO), the Hong Kong Government considered introducing a new subject of “sensitive data,” which would have been subject to more rigorous controls. However, the provision was dropped due to a lack of consensus on the coverage, regulatory model and sanctions for the protection of sensitive data. While the proposed introduction was aimed to protect “sensitive data,” there are already quite comprehensive frameworks available in the Asia Pacific region.

Some jurisdictions provide a higher threshold of protection for “sensitive data” or “sensitive information,” 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.
In June 2015, Singapore launched a National Electronic Health Record System. All Singapore residents are automatically enrolled in the system, unless they have expressly In the context of electronic health data, the main purpose and benefit of having an eHR System is to enable the sharing of such data amongst health-care providers on compliance with the PDPO, both the eHR Commissioner and health-care providers are considered data users in relation to individuals' health data. The EHRSSO and PDPO are intended to be in sync, and are only intended to take effect after a consultation period for the introduction of the eHR System and render it inoperable.

Given this, it was proposed that instead of individuals being able to provide an "all or nothing" consent (i.e., permitting the specific health-care providers accessing all of the data on an individual’s health record), they should also be able to specify certain types of data that would require them to provide separate consents for each type of 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 System, which is to enable the sharing of such data amongst health-care providers. In addition to a provision requiring each person to provide their general 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.

In the end, due to the sensitive nature of health data, the Australian Government may consider switching to a national opt-out scheme from its current opt-in scheme.

The above provisions were agreed by the Legislative Council and are only intended to take effect after a further study and consultation is carried out on how such Specific Consents aren’t yet in operation. 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. The scope and application of the Specific Consent aren’t yet in operation. The scope and application of the Specific Consent aren’t yet in operation.

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 real, due to the sensitive nature of health data, the EHRSSO is intended to address a balance between protecting patients' privacy and the overall aim of the eHR System, which is to enable the sharing of such data amongst health-care providers. In addition to a provision requiring each person to provide their general 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.

In the end, due to the sensitive nature of health data, the Australian Government may consider switching to a national opt-out scheme from its current opt-in scheme.
The PC specifically refers to health records as ‘sensitive personal data’ in the Healthcare Providers Information Leaflet, even though the PDPO does not provide recognition of 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 their consent;
(b) the use of the personal data contained in the eHR System will be controlled by the PC and the Health-care Professional;
(c) patients can withdraw their consent at any time, and health-care providers must explain the impact of the withdrawal of consent to patients;
(d) patients must ensure that their health-care 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;
(e) health-care providers must explain the operation of the eHR System to patients, to ensure that they understand the implications of their personal data being shared on their behalf;
(f) any data breaches should be promptly notified to the eHR Commissioner;
(g) health-care providers must ensure that the health-care service is provided in accordance with the privacy by sharing their health records;
(h) health-care providers should ensure that the 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 access);
(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; and
(j) if the health-care provider receives any data access request from a patient in respect of personal data uploaded onto the eHR System for 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 protect the EHRSSO’s integrity and to reflect the seriousness of the potential misuse of health-care data or of any unauthorised access to the eHR System, the government introduced new offences to the EHRSSO.

Under the EHRSSO, a person commits an offence if:

(a) she knowingly impairs the operation of the eHR System in order to obtain or use unauthorised access to the eHR System;
(b) she makes a false statement for the purposes of enabling a patient to provide his/her consent to the sharing of their data;
(c) she knowingly damages data contained in an electronic health record for direct marketing purposes;
(d) she uses or transfers another person’s data contained in an electronic health record for the purpose of enabling a patient to provide his/her consent to the sharing of their data;
(e) she uses or transfers another person’s data contained in an electronic health record for direct marketing purposes;
(f) she knowingly causes access or modification to data contained in an electronic health record for direct marketing purposes;
(g) she makes a false statement for the purposes of enabling a patient to provide his/her consent to the sharing of their data;
(h) she knowingly damages data contained in an electronic health record (without lawful reason);
(i) she knowingly causes a computer to perform a function so as to obtain unauthorised access to data contained in an electronic health record, or causes the accessibility, reliability, security or processing of such data to be impaired;
(j) she knowingly causes access to modification of data contained in an electronic health record, or causes the accessibility, reliability, security or processing of such data to be impaired.

Most of the above offences can incur a fine of up to HK$ 1,000,000 ($128,906) and/or maximum imprisonment of 5 years, save for a breach of the data protection prohibition which can result in a maximum fine of up to HK$ 5,000,000 ($644,530) and/or up to 10 years imprisonment. The same acts that give rise to one of the above offences, could also amount to an offence under the Crimes Ordinance (Cap. 200) (CO), or the direct marketing of personal data contained in an electronic health record.

The offences under the EHRSSO are broader than the offences under the PDPO. However, the same acts that give rise to an offence under the PDPO 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 made relating to a breach of the PDPO and/ or CO, then the PD and EHR Commissioner both have the power to either refer the complaint to the other for their consideration or decide to investigate the complaint jointly.
thus clarifying that the stricter offence under the EHRSSO in the Healthcare Providers Information Leaflet, electronic health record. This was reemphasised by the any data or information of a person contained in the isn’t expressly limited to ‘personal data,’ but applies to any of the data contained on the eHR System for direct any data subject’s consent, no such procedure applies under the EHRSSO. The EHRSSO makes it an absolute of necessity to be exercised by health-care providers if they decide to disclose patients’ personal data to third parties.

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 computer or methods of committing the offence. Like an offence under the EHRSSO is to cause any damage or to cause impairment of the accuracy, reliability, security or processing of such data, or to cause any damage or to obtain unauthorised access to the data. If health-care providers have personal data stored on their own local systems, the PDPO has stated that they can still use such personal data for direct marketing purposes. However, in practice it may be difficult for a healthcare provider to prove that it indeed the person’s personal data used in its own local system, rather than these electronic health records on the EHRSSO to act as a deterrent against any misuse of health records or the privacy rights and the security of their data.

The offences introduced by the EHRSSO must be a deterrent against any misuse of health records or the EHRSSO provides no specific legal obligations concerning the security measures and guidelines that need to be implemented to prevent cyber-attacks. The EHRSSO mandates that health-care providers, including the eHRSSO, must ensure that all employees are aware and concerned about the data privacy rights and the security of their data.

The offences introduced by the EHRSSO must be a deterrent against any misuse of health records or the EHRSSO provides no specific legal obligations concerning the security measures and guidelines that need to be implemented to prevent cyber-attacks. The EHRSSO mandates that health-care providers, including the eHRSSO, must ensure that all employees are aware and concerned about the data privacy rights and the security of their data.