corehealth

TECHNOLOGIES

Inspire. Ignite. Revolutionize. Well-Being.

Where in the World May Personal Information Be Stored?

Where in the World May Personal Information Be Stored?

DISCLAIMER: The contents of this blog do not constitute a legal opinion. It is based on the most recent information at the time of writing. Readers are advised to seek legal counsel for any issues requiring legal opinion.

Numerous myths and misunderstandings exist related to the geographic location of the storage of personal information or data, particularly sensitive Personal Health Information (PHI). Must it be stored onshore? Can it be stored offshore? If so, in what locations and under what conditions? If the data is physically stored in the country of origin, may it be accessed for support and troubleshooting by someone in another country? What about a remote screen share where the data is not actually crossing international borders?

It seems that no matter who you talk to, in whatever country, you tend to get different interpretations of what the law says about the matter. Read on if you'd like to know our views on the location in which personal information may be stored. Our views are based on consultations with information privacy experts.

United States

If you are a Covered Entity, you are bound by **Health Information Portability and Accountability Act (HIPAA)** and its more recent amendments such as **The Health Information Technology for Economic and Clinical Health (HITECH)** and the Omnibus Rule. All have been released by the U.S. Department of Health and Human Services (HHS) and are enforced by the Office of Civil Rights (OCR).

As a Covered Entity you must comply with the HIPAA Privacy Rule which applies to all protected health information and, if applicable, the HIPAA Security Rule which applies only to ***electronic protected health information***. As stated by HHS, under the Summary of the HIPAA Security Rule, the Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments.

There are no provisions in HIPAA that place a restriction on the geographic locale in which either protected or electronic protected health information may be stored. As a result, when considering where to store its electronic protected health information, a Covered Entity must assess whether the available options allow it to maintain the reasonable and appropriate administrative, technical, and physical safeguards as are required by the Security Rule. Those Covered Entities that have engaged the services of a Business Associate (BA) to manage this function must ensure that the BA is willing to enter into a Business Associate Agreement (BAA) in which the obligations of the Covered Entity are "assumed" by the BA with respect to the safeguards to be applied to protect the electronic protected health information. Covered Entities should be particularly aware of this issue when dealing with Cloud Services Providers and their willingness to advise the Covered Entity in the event of a breach that would trigger the Covered Entity's breach reporting obligations.

Canada

Subject to two very limited exceptions, you may generally choose to store your personal information in any location in the world. The two exceptions relate to personal data held by government institutions in the provinces of British Columbia and Nova Scotia which prohibit the disclosure of the data outside of Canada. However even these prohibitions are subject to several exceptions, but "disclosure" does include remote access to the data from a location outside of the country.

Where an organization is subject to the provisions of the federal Personal Information Protection and Electronic Documents Act (PIPEDA) or provincial health information privacy legislation, it must comply with those rules with respect to the protection of health and personal information from unauthorized access, disclosure, copying, use or modification. The rules are generally very similar and, at a high level require the organization to develop and implement three categories of safeguards to protect personal health information regarding:

- Physical measures (locked filing cabinets, restricting access to offices, alarm systems).
- Technological tools (passwords, encryption, firewalls, anonymizing software).
- Organizational controls (security clearances, limiting access on a "need-to-know" basis, staff training, confidentiality agreements).

As is the case in the U.S., a Canadian organization should ensure that it has entered into an agreement with any third-party service provider it retains to store its data appropriately and manages the data in accordance with the organization's legal obligations.

Notwithstanding the fact that the legal prohibition on the storage of personal data and PHI outside of Canada is very limited, more commonly, Canadian organizations, as a matter of policy, do not permit their personal data and, in particular, their personal health data to be stored in the U.S. due to privacy concerns stemming from the U.S. A. Patriot Act of 2001 which provides the U.S. Government with the ability to access the personal data of Canadian citizens. What people fail to recognize is the similar rights of the Canadian government to access the personal data of its citizens from government or private sector organizations, the fact that the U.S. government may be able to use its powers under the Patriot Act to access Canadian data stored in Canada if it is controlled by a U.S. company and that there are other methods likely to be used by the U.S. government to access data of Canadians.

Europe

The European Commission's Directive on Data Protection (Directive 95/46/EC) went into effect in October of 1998, and, subject to certain "derogations" (exceptions), prohibits the transfer of personal data to non-European Union countries that do not meet the European Union (EU) "adequacy" standard for privacy protection. The European Commission has recognized the adequacy of Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Jersey, the Isle of Man, Switzerland, Uruguay and New Zealand.

The U.S. has a different stance on privacy regulation and has not enacted any specific legislation that would allow it to be deemed “adequate”. Instead, the U.S. Department of Commerce, in consultation with the European Commission, developed a "Safe Harbor" framework to allow individual organizations to comply with the Directive. Only U.S. organizations subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DoT) may participate in the Safe Harbor.

One of the important derogations is the entering into of a “model contract” for the transfer of personal data to third countries. These contractual provisions have been approved by the EU Commission and do include very stringent requirements. Like the U.S. and Canada, consideration also has to be given between the role of the organization transferring the data and that storing it – “data controllers” and “data processors” in EU parlance. There are specific model contracts to be applied depending on the role of the transferor and the transferee.

Some of these requirements may well change with the passage of the EU Data Protection Regulation anticipated to occur before the end of 2015.

Asia

Eleven jurisdictions in Asia now have comprehensive data privacy laws: Australia (amended), Hong Kong (amended), India (new), Japan, Macao, Malaysia (new), New Zealand, the Philippines (new), Singapore(new), South Korea (new) and Taiwan (amended).

Cross-border transfers of personal data are unevenly regulated. Similar to the European Union (EU), some Asia-Pacific jurisdictions, such as Australia, only permit cross-border transfers of personal data where the recipient of the data is subject to a law or binding scheme that has the effect of protecting the information in a way that, overall, is at least substantially similar to that of the Australian Privacy Principles and which affords the subject of the data transferred an enforcement right, or where prior consent is obtained. Unlike in the EU however, it is the organization making the transfer that makes the assessment of “substantially similar” which appears to be a lower standard of concordance than that required for an EU adequacy designation.

Other countries have passed cross-border transfer rules that are not yet in force, such as Hong Kong and the regulations required to implement the provisions in the Singapore Law. In Japan and New Zealand cross-border transfers are not explicitly regulated by law at all. Finally, the very stringent Korean law requires the prior notice and express consent of the individual in order to collect, use and transfer personal information. The notice must separately detail the collection and use of personal information, third-party disclosures (including any cross-border disclosures and disclosures to third-party outsourcing service providers).

Data privacy rules in the Asia region are, for the most part, less stringent than EU standards and if a country meets the EU’s “adequacy” requirements, it is reasonable to assume that it meets those of Asian countries as well. To date, though New Zealand is the only jurisdiction that is considered to have “adequate protection” by the EU.

Middle East

Israel is the first and only country in the Middle East to be recognized by the EU as providing an adequate level of protection for personal data transferred from the EU. The Israeli Privacy Law requires that individual consent or another legal basis be established for the transfer of personal information outside of Israel unless the transfer is to affiliates that are under the corporate control of the Israeli company. There are also comprehensive security rules that include specific requirements for outsourcing activities.

There are no pan-GCC (Gulf Cooperation Council) or pan-Arabic laws governing data protection and privacy. Nor are there any specific national laws or regulators governing data protection and privacy in Qatar, Saudi Arabia and the UAE of the type found in jurisdictions in the EU. The Qatar Data Protection Regulations apply only to financial services organizations licensed by the Qatar Financial Centre Authority (QFC Authority). Personal information may not be transferred to countries outside the QFC unless the recipient country provides an adequate level of personal data protection, the individual has consented to the transfer or another exception applies. Alternatively, organizations may apply to the QFC Authority for a permit for the transfer.

Private sector organizations located in the Dubai International Financial Center (DIFC), are subject to the DIFC Data Protection Law (DIFC Law), but the law does not apply to organizations operating elsewhere within the UAE. Personal information may not be transferred to countries outside the DIFC unless an adequate level of protection is ensured by laws and regulations applicable to the recipients or an exception applies. All country laws, including the U.S.-EU Safe Harbor Program, that have been found by the EU as proving adequate protection are similarly recognized by the DIFC.

Latin America

Data use and creation is exploding in this part of the world bringing with it an emphasis on privacy. There are currently six countries that have in place omnibus privacy laws: Argentina, Chile, Colombia, Mexico, Peru, and Uruguay. Brazil is currently considering data protection laws.

Unlike the European member state laws that are all based on a common directive, the laws in Latin America vary significantly from each other, including with respect to the requirements for transfer of data outside of the country. The laws of Argentina and Uruguay contain restrictions on cross-border transfers to countries that do not provide adequate protection.

The transfer of personal information to countries outside Colombia that do not provide an adequate level of data protection is prohibited, unless the individual has provided his/her express and unequivocal consent to the transfer or one of a narrow group of exceptions applies. However, cross-border transfers between an organization and a service provider that are pursuant to a Personal Data Transmission Agreement do not need to be notified to the individual and do not require the individual's consent. These are in effective third-party services agreements.

If a Mexican organization transfers personal information to a domestic or foreign third party the organization must provide the third party with the privacy notice that was sent to and consented to by the individual. The third party must process the personal information in accordance with this privacy notice and assume the same obligations as those assumed by the organization.

The regulation made under the Peruvian Law provide that cross-border transfers are permitted when the importer assumes the same obligations as the exporting organization. The exporter may transfer personal information on the basis of contractual clauses or other legal instruments that prescribe at least the same obligations to which the exporter is subject, as well as the conditions under which the individual consented to the processing of his or her personal information. Therefore, if a contract is in place, consent or one of the other legal bases provide for under the law to authorize disclosures of personal information outside of the country are not required.

In contrast to the above, the Chilean law contains no restrictions on cross-border transfers.

The laws in the various countries are based primarily on the European framework and data storage may become as restrictive.

The Bottom Line

1. Understand the legal requirements and restrictions, if any, on where your data may be stored;
2. If there are no legal restrictions, make a risk-based policy decision on the acceptable geographic locales;
3. When considering outsourcing of storage services, clearly understand how your service provider proposes to protect the confidentiality and security of your data, as well as the privacy of the individuals to whom the data relates; and
4. Ensure that your service provider contractually commits to implementing these requirements so that you can satisfy your own legal obligations related to protection of the data.

If you have any questions, CoreHealth would be happy to discuss in more detail or recommend a Privacy and Security lawyer who can provide you with legal advice.