Union Internationale des Avocats
International Association of Lawyers
Unión Internacional de Abogados

60th UIA CONGRESS

Budapest / Hungary
October 28 – November 1, 2016

UIA Biotechnology Law Commission
Sunday, October 30, 2016

Hacking Pacemakers and Beyond: Cybersecurity Issues in Healthcare

Cyber Security and Health: Data Fiction and Privacy How EU and Trans-continental treaty (e.g. TTIP and TPP) and international body (e.g. WTO) are facing the challenge

Fabio Marazzi, (Marazzi & Advisors)
via Foro Buonaparte, 51, I-20121 Milano, Italy –
tel.: +39 0272095436 – mail f.marazzi@madv.eu

Union Internationale des Avocats
International Association of Lawyers
Unión Internacional de Abogados

I. INTRODUCTION

New technological developments in the field of healthcare pose a potential threat to privacy rights of consumers and patients and require healthcare providers to implement a number of measures for the adequate protection of sensitive information.

Provision of cross-border services, including healthcare-related services, already represents an integral part of global trade numbers and therefore mandates the importance of implementing further and more detailed measures for data protection at international level.

Vulnerability to Data theft and privacy violation are themes of concern for the consumers and supranational institution such as the European Union, which approved a directive on personal data protection, constituting the basis for the recently approved the Eu Us Privacy Shield as well as a topic considered in international treaties.

The recently adopted text of the Trans-Pacific Partnership (TPP) provides an opportunity for evaluating the status of current global regulation and possible future developments. Indeed, the inclusion of a dedicated chapter (Chapter XIV) purposefully aimed at regulating electronic commerce – including, for the present purpose, consumer protection and privacy - signals the importance of this topic in the context of supranational agreements.

Furthermore, given the absence of specific provisions in the context of multilateral trade agreements (most relevantly the WTO agreements) dealing with health-related privacy issues, and in consideration of the secretive nature of the currently ongoing negotiations of the Transatlantic Trade and Investment Partnership (TTIP), the importance of identifying possible regulatory scenarios for data protection cannot be underestimated.

II. CROSSBORDER HEALTHCARE MARKET

The provision of healthcare services to patient coming from other countries is greatly increasing. In fact, the trend that can be identified also as medical tourism is already valued at 438 Bn. Dollars with a projected rate of increase in the next ten years of 25%. There is an estimated amount of 11 million patients travelling abroad each year to receive medical treatment. The reasons on the basis of this trend are the research for better quality treatments and/or the research of affordable treatments with a good quality. The main medical tourist destinations are United States, followed by Thailand, Singapore, Germany, Korea, and Spain.

The increase in cross border provision of medical services creates new potential dangers for patient data privacy, in fact the main destination are countries with legal different system, different level of economic development and different level of patient privacy protection. Germany and Spain are member of the European Union a supranational entity that has created a set of rules to protect patient data transfer between member countries and to a third country outside the Eu. On the contrary, the other countries are member of different economic blocs. It is evident that due to market development the need of international treaties on patient data processing and privacy is everyday increasing, nevertheless it is important to note that Us and Singapore are between the countries signatory of the TPP agreement that contains provision about data privacy as we describe on chapter 5.

Union Internationale des Avocats
International Association of Lawyers
Unión Internacional de Abogados

III. EUROPEAN UNION, DIRECTIVES ON PROTECTION OF SENSITIVE DATA.

European Union is a supranational entity composed by 28[1] States. Since the nineties it has adopted several regulations in order to protect citizen privacy, and their sensitive data (i.e. health data) also in the context of a digital connected world.

- **DIRECTIVE 95/46/EC**[2]

The Directive contains a set of rules for member States regarding the protection and processing of personal data and the free movement of the same, outlining a different treatment for the processing of data on the basis of the type of data. Indeed, sensitive data, such as health data, are subject to different standards regarding processing.
As stated in Section iii, Article 8: 1. *Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*.
So the general policy is to prohibit the processing (i.e collection, storage, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available of personal data, whether or not by automatic means) of personal sensitive data, thus ensuring a strong protection for privacy of Eu citizens.
Nevertheless, the same article has a provision for exceptions to the general policy, whether:
(a) *the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards;*
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

The Directive thus provide for a few specific exceptions strictly related to the laws of member States concerning privacy of citizen. These exceptions apply only in the cases when the subject gave specific consent or if necessary in employment law or to protect the vital interest of the subject and in two other cases. In addition to it, the general policy shall not apply in case the processing of personal sensitive data is necessary for the purpose of preventive medicine, the provision of care and treatment only where: *those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy*[3].
Another exception to the general policy can be lay down by Member States only in case of substantial public interest and only if suitable safeguards are provided.
The intent of the Directive is to provide to the citizen the maximum protection possible for their health data, generally prohibiting the processing of the same. The exceptions contained are strictly related to the laws of the States regarding the privacy of their citizen, or the reason of public interest, thus providing a

[1] United Kingdom is still a member of the European Union, the so called "Brexit" negotiations are about to start.
[2] Directive of the European Parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[3] Art 8. 3,4

framework of supranational rules for a group of countries with different legal systems, level of economic development and different cultures.

The Directive lays the basis of current agreements between the European Union and the Us regarding the transfer of data, that are described in the following chapter. In fact, Article 25 has a provision regarding the possibility to provide personal data that are undergoing processing or will be processed after transfer, to third countries only if the third country ensures and adequate level of protection[4].
The Directive contains also prescription about the necessary assessment of the level of protection:
2. *The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country….*
If an inadequate level of protection has been assessed, the Member States: *shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.*
The Directive in the article 26 provide for exceptions based on: *the consent of the subject of the data, the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or the transfer is necessary in order to protect the vital interests of the data subject; or the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.*
It is possible to affirm that regarding the transfer of data to third countries, this action is allowed only in case the third country has an adequate level of protection. There are few exceptions related to the specific authorization of the subject, the performance of a contract concluded in the interest of data subject, on the basis of public interest or related to legal claims. Another exception is when the transfer is made from a register which is intended to provide information to the public. In this case is important for the data subject, to consider and analyze thoroughly, the conditions on the basis of which he is giving is consent about the processing of personal data.

- **CROSS-BORDER HEALTH CARE DIRECTIVE AND PRIVACY IMPLICATION ON THE EU CITIZEN**

Several fundamental rights are recognized in the Eu laws for its citizens. The right to receive medical treatment in a country different to the home country, (subject to certain conditions), is one of them. The Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare provide the framework in which cross-border healthcare services can be provided to an Eu citizen. The Directive, is devoted to create a framework to simplify and standardize the procedures to request health care services in other Member States. In addition to it, the document reaffirms the right and principles regarding the protection of medical personal data during the transfer of data between member countries while guaranteeing the flow of the same inside the Union.
In the whereas of the Directive it is stated that: (25) *The right to the protection of personal data is a fundamental right recognised by Article 8 of the Charter of Fundamental Rights of the European Union. Ensuring continuity of cross-border healthcare depends on transfer of personal data concerning patients' health. These personal data should be able to flow from one Member State to another, but at the same time the fundamental rights of the individuals should be safeguarded.*

So, the directive reaffirms the provision about the respect of fundamental rights of citizen while stating that personal health data shall freely flow from one Member State to the other. This flow shall be strictly compliant with privacy right. In fact, as stated in Article 4 2 e)[5]: *the fundamental right to privacy with*

[4] Article 25 Principles
[5] Chapter ii Responsibilities Of Member States With Regard To Cross-Border Health Care, Article 4, Responsibilities of the Member State of treatment

respect to the processing of personal data is protected in conformity with national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC;

The general framework for provision of cross-border healthcare services in the Union is created in order to guarantee the operation of the system also through the free flow of personal health data, with a strong provision related to the respect of fundamental rights of privacy of the citizen. The Directive, being an international agreement even in the context of a supranational Union, is a good example of the need to create international rules governing the transfer and the security of health data at an international level while guaranteeing the flow of them, answering to the need of a health sector strictly interconnected.

IV. EUROPEAN UNION, UNITED STATES OF AMERICA DATA SHARING AGREEMENT

The data sharing agreement between European Union and United States known as Safe Harbors has been struck down by the Court of Justice of the EU on October the sixth 2015. The regulation, developed in the nineties provided a framework for transferring personal data from the Eu to the Us that, as ascertained by the Court ruling, didn't guarantee the Us had a privacy level similar to the level provided in the Eu regulations, a right of an Eu citizen in case of data transfer to a third country. This ruling was made after it was revealed that in 2013, US used a mass surveillance system on Eu citizens. To restore transatlantic trust and to create a new framework for data exchange, the Eu negotiated a new agreement known as the Eu-Us Privacy Shield.

- EU US PRIVACY SHIELD, MAIN PRINCIPLES[6]

The EU-U.S. Privacy Shield is based on the following principles: Us organizations in order to transfer data from Eu to Us in compliance with the regulation must self-certify to the Us Department of Commerce with the adherence to the Principle of Privacy Shield.
In particular an Us organization:
- must be subject to the investigatory and enforcement powers of the Federal Trade Commission (the "FTC"), the Department of Transportation or another statutory body that will ensure compliance with the Principles;
(b) publicly declare its commitment to comply with the Principles;
(c) publicly disclose its privacy policies in line with these Principles; and
(d) fully implement them. An organization's failure to comply is enforceable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. § 45(a)) or other laws or regulations prohibiting such acts.
The Us Department of commerce committed itself to create, update and make public a list of Us companies that choose to comply with privacy shied: *the adherence to the Principles may be limited by to the extent necessary to meet national security, public interest, or law enforcement requirements*.
The new regulation tackle also the problem of mass surveillance by the Us on Eu citizen. In fact[7], *the US has given the EU assurance that the access of public authorities for law enforcement and national security is subject to clear limitations, safeguards and oversight mechanisms. Everyone in the EU will, also for the first time, benefit from redress mechanisms in this area. The U.S. has ruled out indiscriminate mass surveillance on personal data transferred to the US under the EU-U.S. Privacy Shield arrangement.* The Office of the Director of National Intelligence further clarified that bulk collection of data could only be used under specific preconditions and needs to be as targeted and focused as possible. It details the safeguards in place for the use of data under such exceptional circumstances.

---

[6] Source http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf text written in Italic is taken directly form the text.
[7] European Commission - Press release: EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, Strasbourg, 2 February 2016, retrieved form the intenet

The regulation creates a standard for the treatment of personal data, distinguishing between general data and sensitive data, such medical or health conditions[8]. In fact, if for general personal data:
2a) An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals.
For what concerns sensitive information organizations must:
2b) obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive

This is particularly relevant for the topic of patient privacy, in fact the agreement, as reported above, provides for a stricter treatment of sensitive and health information, compared to personal information. An express consent (opt in) is requested in case sensitive information while, just a choice, (opt out) is provided in other cases.
Nevertheless, the agreement contains provision regarding exceptions to the general mechanism of express consent (opt in) for sensitive Data: *III 1 a. An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is: i. in the vital interests of the data subject or another person; ii. necessary for the establishment of legal claims or defenses; iii. required to provide medical care or diagnosis….*
Exceptions are based on vital interest of the subject, legal claim of defense and for providing medical care or diagnosis. This article, is extremely important to enable cross border telemedicine and healthcare service supply, guaranteeing the flow of personal health information necessary to provide medical care or diagnosis.

.

V. TPP

The Trans-Pacific Partnership or Tpp has been signed by 12 countries of the Pacific, namely: Australia, Canada, Japan, Malaysia, Mexico, Peru, United States, Vietnam, Chile, Brunei, Singapore New Zealand and United States. The main goals of the agreement are: establish comprehensive regional agreement that promotes economic integration to liberalize trade and investment, bring economic growth and social benefits, facilitate regional trade by promoting efficient and transparent customs procedures that reduce costs and ensure predictability for their importers and exporters. The Tpp comprises also a chapter aimed at regulating electronic commerce as well as the acceptance of electronic signature and authentication between the citizen of signatory parties; signaling the importance of this topic in international agreements in a digitalized and interconnected world.

In particular, article 14.6 confirms the validity of electronic authentication and electronic signature as means of realizing transactions stating that: *except in circumstances otherwise provided for under its law, a Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form*. The agreement states also that the Parties can't adopt or maintain measure that would: *(a) prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction; or (b) prevent parties to an electronic transaction from*

[8] Eu-U.S. Privacy Shield Framework Principles Issued By The U.S. Department Of Commerce, annex ii, paragraph 2 a); 2 b).

having the opportunity to establish before judicial or administrative authorities that their transaction complies with any legal requirements with respect to authentication[9].

So the first part of article 14.6 binds the signatory parties in enabling the possibility of electronic signature and authentication. The article prohibits also measures preventing the possibilities for the parties, to establish before judicial or administrative bodies that their transaction complies with legal requirements regarding electronic authentication. By consequence, the TPP provides for a "liberalization" of electronic transactions based on electronic authentication complying with legal requirements.

What is more relevant, in my opinion, relating to cybersecurity and data privacy is article 14.6 paragraph 3. The article states: *notwithstanding paragraph 2, a Party may require that, for a particular category of transactions, the method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its law*.
This article provides the signatory parties with the possibility to establish certain performance standards or certifications by authorities accredited, for certain category of transaction. This is in my opinion the main possibility for Governments, lawmakers and stakeholders to cooperate in order to establish common framework on a supranational basis to protect patient and citizen data in electronic transaction exchanges, guaranteeing privacy and security while enabling operators to exchange data need to fulfill their activities.

The TPP contains also paragraphs relating directly to personal information protection, binding the parties to adopt specific measures to protects personal information because of economic and social benefits of protecting the personal information of users of electronic commerce. In particular the more relevant article regarding personal information protection is, in my opinion, the 14.8 (2) note 6. The article states: "*for greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy*".
So, the parties that have to comply with the obligation relating to personal information protection can choose between adopting law regarding privacy or laws that provide for the enforcement of voluntary action by enterprises.

Another relevant element of the Tpp is the article 16.6 that promotes the cooperation and coordination *on matters of mutual interest related to fraudulent and deceptive commercial activities* including *cooperation with respect to online commercial activities*, as stated in article 14.7. This is extremely important in fact a greater cooperation and coordination between relevant national public bodies in these matters is one of the key answers to protect consumers in the signatory countries, without leaving room for malicious and fraudulent activities realized thanks to difference between countries laws and no cooperation between national public bodies.

VI. TTIP

The Transatlantic Trade and Investment Partnership, or Tttip, is a trade and investment agreement, whose negotiation started in July 2013 between the European Union and the Usa. The negotiate is not public and what is available is actually only the mandate and statement by the Eu negotiator at the conclusion of negotiation rounds, in addition to an information website.

On Sunday Agust the 28th German Vice Cancellor and Economy Minister, said: "In my opinion, the negotiations with the United States have de facto failed, even though nobody is really admitting it". By that, negotiation seems to have failed and the parties didn't agree on a single chapter of the negotiation.

[9] Tpp Chapter 14, Electronic commerce; Art. 14.6, 2; retrieved from the internet.

From the latest available information, data protection standards haven't been part of Ttip negotiation. E-commerce will be one of the topic object of the Ttip, but no specific information are available.

VII. CONCLUSION

Nowadays topics such as data privacy, cybersecurity and data protection are becoming extremely important issues, in particular in the healthcare sector. In fact, the increasing provision cross-border healthcare services, a market valued 428 Bn. US Dollars, the integration of countries in economic or political blocs and the general will to increase the pace of liberalization of trade in goods and services affects the patient data protection online and offline.
Several Government adopted national law on privacy, cybersecurity and health data privacy. Nevertheless, there has been and there is an urgent need of international treaties on these topics. As we reported there are not common regulations at the Wto level, so international treaties have been limited to political Unions or trade blocs.
European Union recognizes to its citizens several fundamental rights; between them, the right to the protection of personal data. In order to ensure the respect of this right the Commission and the Parliament adopted the directive 95/46/EC. The Directive contains the general rules related to the processing of sensitive personal data of European citizen whether or not by automated means inside the Eu and about the transfer of those data to third countries.
In addition to it, to establish a set of rules for cross border healthcare inside the Eu, the Directive on cross-border healthcare has been approved. This directive not only provide for a common framework, in which the Eu citizen can move from their home country to another Member country to receive healthcare treatment, but also guarantee the free flow of patient information subject to provision of privacy law.

Following the provision of directive 95/46/EC concerning the transfer of personal data to third countries the Eu signed agreement with the Us. The recently adopted Privacy Shield represents a step forward in guaranteeing the protection of privacy rights of citizen. In fact, while giving the possibility to organizations and companies to collect personal and sensitive data, the regulation defines two different treatment regarding the choice and consent to provide data. Even if some issues remain not completely solved (such as the ones related to surveillance or national interest) Privacy Shield provides citizens new instruments to protect themselves and to file claims if there has been a violation of their rights. Indeed, they can file complaint to the company violating their rights or use free of charge Alternative Dispute resolution (ADR) or file complaint to the national Data Protection Authorities.

The Trans Pacific Partnership is an agreement between 12 countries of the Pacific rim of utmost importance. The Tpp agreement is essentially a trade and investment deal drafted and signed with the goal of increasing the liberalization of commerce between the signatory countries reducing cost and bringing social and economic benefits. What is relevant for the discussion topic is the chapter XIV that contains provision regarding electronic commerce. Coherently with the goal of the Tpp, the text provides for a liberalization of electronic transaction based on electronic authentication complying with legal requirements. The Agreement, nevertheless provide the parties with the possibility to create national regulations, standards and certifications to be applied on certain categories of transactions. So, the agreement recognizes that the methods of electronic authentication may be chosen by the national Governments, while encouraging the interoperability of the same. The Agreement recognizes the value of national regulation on data protection and privacy protection. In fact, it contains a provision encouraging the Parties to adopt or maintain measures such as privacy laws, data protection laws or the enforcement of voluntary standard by companies relating to privacy. Another relevant content of the agreement is the article 16.6 that promotes cooperation and coordination on matters related to fraudulent and deceptive commercial activities also online.

TPP is a good example and a good starting point for further agreements between countries relating to trade, investment but also to electronic commerce and data privacy. In fact, while it encourages further liberalization and reduction of barriers it reaffirms the important of cooperation between national Governments and authorities on topics such as data protection, privacy protection and prevention of fraudulent and deceptive commercial activities also online, in order to respond to the necessities to citizen-costumer.

An international treaty based on cooperation between national Governments shall be main goal of undergoing negotiation regarding Ttip. Nevertheless, there is still the need of a general agreement on data privacy, in particular relating to medical data, to be used by the healthcare provider and to protect citizen rights. Cross-border healthcare involves several countries member of different political and trade bloc so, in order to reach a common standard of protection and cybersecurity, it is necessary to reach a deal with the greatest number of countries possible, also leveraging on the international treaties already existent. The best solution would be a general agreement negotiated at the Wto in order to reach an agreement between the maximum number of countries, guaranteeing the protection of privacy and security, facilitating also through this mean an expansion of commerce and investments in healthcare sector.