Impact of GDPR on the Health Insurance Business
Petra Wildemann
23. April 2018

The closer we get to the new GDPR terms, the more we learn what impact this will have for different industries. Organizations need to prepare themselves to be ready to comply with the new General Data Protection Compliance Regulation. More than a regulation, GDPR is a paradigm shift which forces industries to think differently about personal data and how to protect all elements of personal data. The regulation applies to all companies in the EU and abroad whenever data is processed on EU data subjects.

GDPR challenges all industries. However, it has a special impact on the healthcare business because of the large role that personal data plays in healthcare. "Personal" data is defined as "all information, which is related to a natural person", including name, identification number, location data, and all information with respect to the health, culture identity and social identity of a person.

The effects of GDPR on the healthcare business will be huge. When technology started to be used in doctor's offices, it seemed to be obviously a really good idea to use global support for medication, treatments or special analysis around the world. With technology, doctors are able to obtain a second or third opinion just by sending data to experts, who may be far away, for review. This process is much cheaper than flying the patients to specialists or having the specialists fly to patients.

With the new GDPR terms in place, the patients need to agree and approve the process of sending personal data outside of the doctor's offices when obtaining results not only on life-threatening diseases but also on procedures as simple as blood-tests.

As outlined in the PEGA definition, GDPR contains three additional, important definitions that pertain to health data:

1. "Data concerning health" is defined by the GDPR as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."
2. "Genetic data" is defined by the GDPR as "personal data relating to inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."
3. "Biometric data" is "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."

This process and the definitions imply that each healthcare organisation, from doctors' offices to healthcare business organisations, have to use "data officers" when transferring health data either locally, internationally or via cloud storages. Healthcare professionals include not only doctors, nurses and pharmacists, but also health insurers, hospitals and

what are called “cloud- or cyber-doctors”, when medical analytical services are provided cross-border. The more technology is used in connection with healthcare services, the higher the risk that personal data that personal data will be improperly accessed.

Although the GDPR is an EU regulation, it will also force non-EU countries to change their data-protection practices. Personal data transferred cross-border from the EU to, for example, U.S. organizations, will have to be secured by those U.S. organisations in compliance with the new regulations, even if they are stored in a U.S.-based cloud. Whenever healthcare data are exported from the EU, additional concerns, conditions and obligations for the health care industry will be triggered.