NJORD Estonia: How to protect personal data in health care institutions?

It doesn't matter whether the healthcare provider is a general practitioner, a dental practice or a private clinic, all of them need to ensure the confidentiality of the personal data of their patients. It must be thereby considered that the medical sector processes health data containing special categories of personal data, which must be processed confidentially as required by law and the clients.

1. Check what kind of agreements and under what conditions the agreements have been concluded with the cooperation partners and the employees
All agreements concluded with the service providers and cooperation partners must be analyzed and mapped. A healthcare service provider must guarantee secure processing of personal data by the cooperation partner. It must be unambiguously clear, what is confidential information and how that must be treated. The healthcare service provider must be sure that in case of a data breach, a claim can be filed against the agreement party. If the agreement does not provide liability clauses, then the only way to claim something from the counterparty is through the civil liability proceedings, which, as a rule, require a major burden of proof from the claimant in the legal proceedings. The agreement with the cooperation partners must provide assurance for the healthcare service provider that the cooperation partner is aware of what he is doing. In case an incident occurs, caused by the cooperation partner or with his knowledge, then it is important that the cooperation partner knows when and how to notify the healthcare service provider.

The employees should also not be neglected. Firstly, employees must know how personal data should be processed and what kind of data is confidential. Secondly, the employees, when communicating with cooperation partners, must know what to request from the cooperation partners and what to notice when concluding agreements.

2. Find out what kind of data is collected and where the data are stored
Each organisation must know what kind of data they need for providing the service and on which grounds the data may be collected. Collection of all data is not reasoned if it is not needed in practice. It must be considered, though, that there must be a legal basis for the collection of data: (i) is the obligation of the processing of data provided by law, agreement or the data subject's consent? If the required data are mapped, it must also be mapped, where such data are kept and whether the data storage methods are secure. Special consideration should be given to when and how the data shall be destroyed.

3. Prepare the internal rules of the processing of personal data for the employees and the privacy policies for the patients

All rules of the processing of personal data must correspond to reality. It means that the rules of data processing cannot differ from the real situation (i.e. according to the procedure all is secure and fine, but, in reality, there is no overview of who and when gets access to what kind of data and how data are processed). The external persons must also be able to examine the rules, on the basis of which the health service provider processes personal data. Therefore, privacy policies for clients must be drawn up.

4. Crosscheck the agreements and the consents taken from the patients
Agreements for providing healthcare must also include provisions on personal data. It is important to know thereby that it is not enough to include only the clauses „all data is confidential" or „hereby you give your consent to the processing of your personal data". Check whether the conditions of the processing of personal data agreed with the patient correspond to reality and how the amendment and transfer of data and „the right to be forgotten" can be applied.

5. What to do if data still leaks or is held hostage?
Incidents cannot be 100% foreseen and avoided. However, practical steps can be developed in time on what to do and who to inform, both, internally and externally, in case something has happened with the data which should not have happened. The chain of command regarding the movement of information and the further orders must be clear, as serious damage could be done to a small general practitioner as well as to a large hospital if the incident were to be mishandled.

6. Check whether a Data Protection Officer should be appointed
GDPR provides the conditions under which the organisation must designate a data protection officer. As the main activity of a health care provider is related to the processing of health data, it probably must appoint a Data Protection Officer. Even if the healthcare provider must not designate a data protection officer, they should find an advisor, who can give daily prompt advice on personal data issues.

7. Train your employees
Most of the problems related to the processing of personal data arise from the fact that the employees are not trained in the principles of personal data processing. The organisation may have drawn up comprehensive documentation, but often the employees have not examined them. Situations, where incidents occur due to ignorance or negligence, must be avoided. Practice the situations with the employees to make sure they know what kind of information they may reveal by phone, what kind of information they may discuss in the presence of a patient, how to identify a person, what may be disclosed to the relatives.

8. Determine and arrange regular compliance checks to identify and fix problems
Data protection must be attended to constantly. It is important that all rules of procedure are regularly reviewed and employees trained. If necessary, carry out data protection impact assessments to verify what hazards may exist or occur.

LIISI JÜRGEN
ATTORNEY AT LAW,
PARTNER

(+372) 66 76 440
LIISI.JURGEN@NJORDLAW.EE