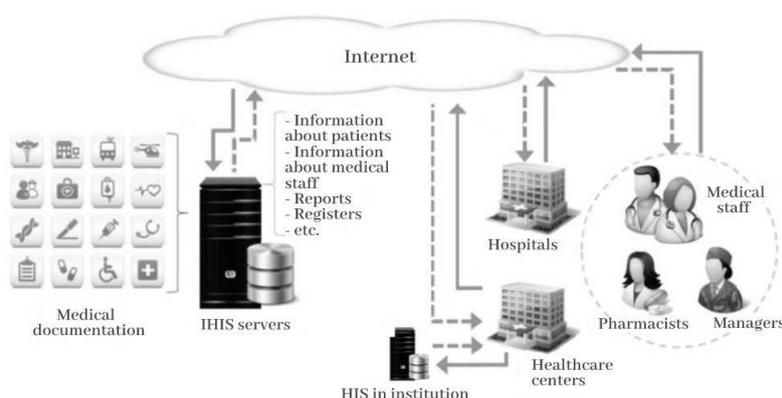


Performance Audit Report
“IT Security in Healthcare Information Systems”

Ministry of Health, Institute of Public Health of Serbia "Dr. Milan Jovanović Batut" and Vojvodina Provincial Secretariat for Health should enhance their information security measures, which will contribute to better reliability of healthcare information systems in the Republic of Serbia

Integrated health information system (IHIS) was introduced during the course of 2016 and consists of a health-statistical part and health information systems used by healthcare institutions, such as Heliant, NextZUS, ZIPsoft, etc.

Databases in these systems collect sensitive personal data, which requires the use of certain protection measures. The previous audits of health information systems have identified a number of issues relating to information security, in several areas: access to database by the service provider, ways of registering the insured person in the system, management of backup copies, disaster recovery plans, inadequate IT organizational structure, obsolete equipment, etc.



It is necessary to enhance the **management** of information systems, primarily through the adoption and use of strategic documents and accompanying financial plans that should ensure sustainable functioning and development of these systems, through the establishment of a clearly defined organizational structure and through proper definition and application of appropriate rules and procedures and effective management of IT risks.

For the reliable functioning of all components of IHIS (which covers all individual systems in institutions), it would be necessary to adopt and implement **business continuity** plans in emergency situations, whose integral part is management of backup copies, in line with legal obligations, followed by periodic testing of such plans.

Ensuring data availability, confidentiality and integrity are the essential goals of IHIS, which is why it is necessary to undertake measures toward their achievement. This requires the adequate organization of **IT security**, adoption of rules and procedures in this area, regulating the process of service provision contracting and establishment of the reliable system of data input and handling of output data.

Recommendations

After conducting the audit, some of the recommendations issued by the State Audit Institution to its auditees, are the following:

To the Ministry of Health, to:

- undertake activities in terms of preparing the proposal of the Strategy for development and organization of integrated health information system and the Action plan for the implementation of the Strategy, and when preparing financial plans, to ensure sustainable financing of goals foreseen by the Action plan for the implementation of the Strategy
- specify the requirements for the functioning, management of risks and security of information systems, including business continuity planning

To the Institute “Batut”, to:

- regulate the process of data processing by the service provider in health information systems in a manner stipulated by law, which involves the mandatory use of data protection measures, and may include the certification process and provision of specific or general written authorization to other data processing entities.

To Vojvodina Provincial Secretariat for Health, to:

- when preparing the financial plans, ensure sustainable financing of goals foreseen by the Action plan for the implementation of the Strategy through detailed planning of funds for development, procurement and maintenance of information systems in the healthcare sector.