Proceedings of 2013 International Conference on
Technology Innovation and Industrial Management
29-31 May 2013, Phuket, Thailand

SUPERVISION AND PROTECTION OF E-DATA IN SENSITIVE INFORMATION SYSTEMS

Red. prof. dr. sc. Vladimir Šimović, Media University, Croatia
simovic.vladimir@yahoo.com

Matija Varga, mag. inf. univ. spec. oec., Media University, Croatia
maavarga@gmail.com

Doc. dr. sc. Marin Milković, Media University, Croatia
dekan@velv.hr

ABSTRACT

The paper shows the possibilities and ways to protect e-data in sensitive information systems such as financial information system and health information system. Nowadays, when the health information system and financial information system are developed and contain large amounts of data in the database, it is necessary to pay great attention to computer security, computer security mechanisms which enable the protection of electronic data, e.g. patient's diseases and clients' financial transactions. The aim of the paper is to present the best way of protecting e-data in the database from malicious people, i.e. malicious users of these systems, and from the deterioration and obsolescence of data storage media with the data important for the organization itself by making recommendations and showing the ways of their protection. This paper, among other things, explains the reason for creating a code of ethics for medical and health IT professionals. The information collected by using the questionnaire is shown. On the basis of this information, it can be concluded that most organizations use scanners and cameras to digitize documents, which are then usually stored in .pdf, .doc, .docx, and xml formats. The results of the research, which was conducted during the period of three weeks in 2012 on the sample of seven organizations, show that there is no organization that does not have a general policy of preserving the material in electronic form. A recommendation for the organizations is made in the conclusion – to back up electronic databases more often, or as many times as possible in the shortest period of time possible. The research presented in this paper, when it comes to collaboration in the development of the programs intended for preservation, shows that the most common form of collaboration is of local character.

Key words: sensitive information systems, financial information system, health information system, electronic data protection, database, methods of saving records.

INTRODUCTION

The paper shows the possibilities and ways to protect e-data in sensitive information systems such as financial information system and health information system. Nowadays, when the health information system and financial information system are developed and contain large amounts of data in the database, it is necessary to pay great attention to computer security, computer security mechanisms which enable the protection of electronic data, e.g. patient's diseases and clients' financial transactions. It is necessary to direct the end users of these

information systems when using health information systems and financial information system to the benefits that such systems provide. The users of such systems should be warned and use preventive measures so as not to abuse or use such data for the acquisition of personal gain at the expense of other clients or patients. The data relating to the case history of a person must be kept secret over the long term. Continuous implementation of the methods of preserving electronic records in the database of health organizations is necessary.

The aim is to present the best way of protecting e-data in the database from malicious people, i.e. malicious users of these systems, and from the deterioration and obsolescence of data storage media with the data important for the organization itself by making recommendations and showing the ways of their protection.

Paper tasks

The tasks set on the topic of "Supervision and protection of e-data in sensitive information systems" are as follows: to point out the possible dangers and threats for clients and patients who make part of the financial and health information systems; to show the possibilities of protection of the patient's and the client's electronic data; to advise on how to use the financial and health information systems; to influence the users of the financial information system and health information system in order to reduce the sensitive data leakage to the closer public; to mention and present the process of migration and preservation of electronic records; to state the reason for creating a code of ethics for medical and health IT professionals; to describe which combination of signs an optimal or strong password which will protect the electronic information system should consist of; to present systems for the supervision and control of the data flow in these information systems. Other tasks of the paper are to explain why it is needed and necessary to evaluate the health information system; to explain why it is necessary to secure the health information system from data loss; to explain who can change the data; to explain how the data confidentiality is realized in the health information system; to explain the functioning of the public health information system and financial information system; and to research which methods, procedures, modes, record formats, input devices, output devices and input-output devices are used by the observed organizations for the preservation of physical documents and records, and electronic documents and records.

Research methods used

For the paper entitled "Supervision and Protection of e-data in sensitive information systems" the following research methods will be used: survey, direct observation method, observation method, analysis, i.e. the method of content analysis, modeling, and interview. In the research methods of the survey and the interview, a sample consists of seven organizations – three organizations are engaged in public activity, two of them are privately owned, and two are educational organizations. This paper will further explain the protection of e-data in the health information system and the financial information system. The process of research using surveys and interviews lasted three weeks and was conducted in 2012. During that time the data on these organizations was collected. The results of the questionnaire data processing are shown by using figures.

THE PROTECTION OF E-DATA IN THE FINANCIAL INFORMATION SYSTEM

People with bad intentions find crashing into the financial information system most interesting. This is because financial institutions have large sums of money in their accounts. However, as the most of the IT professionals who deal with security of information systems claim, an intrusion into the financial information system has not been recorded. Moreover, no case of crashing into the financial banking information system has been recorded. The financial information system is under attack daily, but there are no major difficulties or more serious consequences of malicious people's crashing attempts.

Frequent audits and testing the system's permeability ensure a continuous increase in the security level and implementing the measures to reduce IT risks. At the level of the banking system, there are authorities which collect data about the most common attacks and incidents, and accordingly inform all the participants and require improvement of the system. In Croatia, hacker attacks are not as frequent as in the USA, and one of the reasons is a different language area (Bonić, 2011).

SQL and electronic data protection

SQL is a commercial query language for working with a relational database. Relational databases provide the greatest flexibility in data decomposition, which ensures a great advantage in planning the data distribution on individual system nodes. The standard structured query language is the most popular, best known and most widely used language. It is used to manipulate and manage data contained in the database. SQL server is a product and is closely linked to other servers and layers in a typical IT environment, which is based on the foundations of companies whose databases are in the question. The server is now not only used to store information about users. SQL server is extremely important because the work itself becomes more economical and much easier with it. There are several ways of protection in the SQL Server environment. One way is to provide an additional layer of security for sensitive data. Another way is to follow the rules, standards and laws related to data protection. The third way is related to the protection of the server objects on which the confidential user information and passwords for accessing linked servers can be found. The fourth way is to provide a controlled mode to define privileges for those modules that contain the code. SQL Server 2008, for example, enables encryption of all the data in the database by encrypting the pages of files that contain the database.

When it comes to the processes for managing data integrity, they should ensure accuracy, correctness, completeness or integrity of data in the database. Data integrity on SQL Server can be achieved by using certain constraints and triggers. Constraints are rules that apply to relations. This constraint defines the values allowed to be entered into an appropriate relation and to which range. In many applications, the rules for the preservation of data integrity are defined. However, it is not enough just to define the rules for the preservation of data integrity in an application, i.e. the interface available to the user, but appropriate constraints at the database level should be defined so that invalid data is not entered. The types of data integrity are entity, domain and referential. Entity integrity ensures that each type in a relation can be uniquely identified by a column. It is provided in SQL by using an index which is used to verify the existence of duplicate values. Primary key and constraints which are needed for uniqueness are applied when securing the entity integrity. Primary key and unique

constraints are quite similar and ensure that duplicate record in a relation does not happen. The differences constraints when using a primary key and a unique are as follows: (1) a table can contain one primary key, but X unique constraints can be defined in the table; (2) primary key can not take the null value, while the unique constraint can be defined for the column where the null values are allowed; (3) unique constraint does not use non-clustered index, while primary key uses clustered index. Domain integrity refers to the determination of allowed values for each column of the table. The type of data to be applied to a column in a relation presents one of the ways to ensure the domain integrity. With the domain integrity, CHECK constraint enables the restriction of values allowed in a column based on a logical attribute. Restricting by a foreign key the values allowed in the column are defined, but based on the content of the primary key. Domain integrity can be achieved through procedures, too. Referential integrity ensures and implements foreign or external key and CHECK. CHECK constraints can reference a number of columns in the same relation using the corresponding logical attribute. CHECK constraint can be a part of the create table command or it can be added to an already existing table. After the CHECK constraint is added to an existing table with data, it is checked with regard to the condition defined by CHECK constraint. If in a certain column we have much data, adding the CHECK constraint for that table can last for a while. In SQL, there is a way to skip data check when creating the new CHECK constraint into the existing table. The skipping is done with NOCHECK option. The constraint with a foreign key references the primary key, usually in the second relation in order to preserve the relation (of the weak entity). Referential integrity can be ensured procedurally by using triggers. External key constraint implies the following rules: for each record in the Buyer table there must be the corresponding record in the table Remaining_Part_Document; for each record in the tables Seller and Mark_document there must be the corresponding record in the table Remaining_Part_Document. Entering customer records with incorrect type of identifiers can undermine constraints related to the primary key, and the result is usually an error. Records in the Remaining_Part_Document can be removed if they are referenced by the records in the tables Buyer, Seller and Mark_document. The primary key of the record related to the remaining part of the document cannot be updated if there are records relating to the buyer, seller and mark of the document that it is referenced by.

The constraint with external key may enable the operations of cascading updating and deleting in interrelated relations. The operation of cascading deleting of the record should be used with caution. Deleting a single record can lead to the deletion of a large number of dependent blocks based on a series of tables and relations that are interrelated with foreign or external keys. In SQL, there are four options of settings which are related to the execution of cascade updates and deletions of a foreign key: a SET NULL setting; a SET DEFAULT setting; a NO ACTION setting; and a CASCADE setting. DML triggers are also a means of preserving the data integrity. Triggers allow defining more complex rules to preserve the data integrity in relation to the methods of declarative defining of the integrity and require additional calculations. Triggers are used for preventing faulty commands such as insert, update, and delete, when displaying user-defined messages of an error occurrence and during cascading changes in related tables in a database which cannot be achieved by using the external key.

The protection from an unauthorized access to the e-database

Databases must be protected from an unauthorized access. In addition to physical protection, there is a software mode of protection, where the software is installed in the system for database management. It limits the work with the database, i.e. the work of users who have physical access to a computer or computer terminals. There are several ways to protect databases, such as user identification, various mechanisms of protection, and authority. When it comes to protecting the database by user identification, it is known that each database user has his or her own *username* and a *password* known only to them. The user must present a valid username and password in the system for database management, thus proving their identity. If the user fails to enter a user name and password that correspond to the list into the system for database management, the system for database management refuses to give permission to work with the database. A large number of the systems for database management can be controlled via the Internet. Database can also be accessed from the remote computer, which can be located anywhere in the world. This advantage is also a disadvantage because it opens another door for malicious people to get unauthorized access to certain data. How to protect the database which can be accessed on the Internet? Temporarily, it can be protected by turning off the network system capabilities for database management. Thus, only local users (developers) could access the database, i.e. local network clients. The access to the database may be allowed only to some external users, but only with the identification of the client using encrypted communications such as *ssl/ssh*, double keys, etc. As for the *views*, the user may be given the right to access only a certain part of the data. Other parts of the database are unavailable for a particular user.

Protecting the database by giving authorization defines what the user can do with the data from the database, which is at disposal. The authorization for the protection can be *read/select*, *update*, *insert* and *delete*. The database management system must "memorize", i.e. have a stored list of authorizations for every user and every relation from the specific views. If the user attempts to perform an activity he or she is not authorized of, the database management system will not perform it, but it will print out a warning that the user is not authorized to perform these activities. In most cases, a developer or database administrator is responsible for the protection of the database. Database administrator has a list of users, gives the possibilities of views, and regulates authorizations. Regular users do not have the possibility of regulating the authorities, but only the database administrator. The database should be properly supervised; the changes to the data should be analyzed according to the periods; and the actions of a person who wants to cause harm should be recorded. The functionality of the database management system can also be an indicator of its safety. Back ups or safety copies can also protect the data in the database. Nowadays, you can also use systems that automatically create a back up copy and system recovery, enable data archiving for more than five years, and eliminate the costs that are caused by human error associated with data storage. This type of protection provided by the systems for automatic back up and recovery system is better than backing up an entire database since the system returns only the data that have been changed.

The case of damaging the database and its recovery

With regard to the financial information system, numerous processes are present. The most common of them are purchase, sales, accounting, treasury, and travel warrants. Each of these

processes has its own sub-processes and activities at a lower level. The organizational structure of a certain organization is adapted to these functional areas, as well as jobs on the basis of which profits are generated. Damage to the database in the financial information system may arise due to the failure of the computer hardware (disc and other storage media) or due to an error in the systematic program support. The database may be damaged by the activity of malicious persons (called hackers), accidentally or unfortunately. Malicious people are most interested in the financial information system because e-money is present in this system.

Regardless of the causes and reasons of damage, the database must be returned in the condition of the preserved physical integrity. Under the database integrity we mean truthfulness and accuracy of information or data contained in the database. Problems with the integrity of the database in a broad sense cover all the protection measures whose aim is to prevent the entry of invalid data in the electronic database. Errors which occurred when entering or updating are responsible for the failure results in the base, while the software and system errors are the result of intentional input of invalid data to corrupt the database. The database is protected by constraints. Integrity rules present constraints of the database content for allowed conditions which provide mutual alignment of data of the database while entering, updating and deleting the data. Financial organizations work with the data available to them and in accordance with them, they make very important decisions. The consequences are serious if the data used in the finance department are not correct or have been changed by a malicious person or an attacker.

In order for the database to be restored, prior safety storing of the data from the base to a medium that is located outside the database is necessary. Therefore, the back up of the entire database is done periodically to a special medium, and all changes to the data in the database are recorded in the diary of changes (Varga *et al.*, 2007). On average, data back up from the base to a medium of a company is done by some companies every five days.

THE PROTECTION OF E-DATA IN THE HEALTH INFORMATION SYSTEM

Electronic data in the health information system should be protected from an unauthorized modification or alteration of data, destruction or disclosure of data by reading. When it comes to protecting electronic data in the health information system, family medicine doctors now have a problem with the applications which they use to access electronic data. Problems of applications for the health workers are as follows: (1) non-existence of compatibility between the licensed programs, which sometimes results in data loss during the transition to another application, i.e. a future information source. Doctors of family medicine and those who specialized in other fields today would need to participate more through their professional and expert associations in the evaluation of the quality of the programs (software) they work with. This could contribute to the quality of program functionality and it could be a guarantee that in the future, the program will be fully functional and applicable.

One of the tasks that users and maintainers of the health information system have is to assess system security, data integrity, protection and confidentiality of the data, with the purpose of a more efficient protection of the health information system and the increase of safety.

Electronic database access and the records in healthcare

In the electronic database of the health information system, the data can be accessed via the local workstation, i.e. using the terminal. Moreover, when we consider the application of the health information system, the data can be stored through the local workstation in the SQL e-database, which is located on the Windows 2008 Server. When the data is stored in the e-database, they can be accessed with a specific permission through different terminals, i.e. working places. When a physician works with a specific patient, he or she can access the data of the patient assigned to him, and the physician writes history on his computer, checks for previous diseases in the database, and stores and records the current condition of the patient in the database.

Some of the names of electronic records are as follows: EHR – electronic health record, EMR – electronic medical record, EPR – electronic personal record. The purpose of electronic records in health lies in the possibility of quick and reliable access to the data by health professionals. Such electronic records allow easy storage and the use of electronic data. Electronic health records enable easier function of monitoring the quality of work and administration. Records in electronic format enable faster and easier access to medical and clinical knowledge; they accelerate decision-making process; they indirectly facilitate communication with health insurance. Electronic records enable secure exchange of electronic data with other health organizations. For the physician, records in electronic form facilitate him or her getting to know the patient during his or her illness.

The ways of electronic data protection in health and recommendations for password setting

There are three basic ways of data protection in health: technical means of protection relating to the protection of computer hardware and software; legal means that relates to compliance with the Personal Data Protection Act, the Data Confidentiality Act, the Electronic Signature Act and the Telecommunications Act; and ethical means of data protection. Technical means of protection is ensured by the physical protection of the data carriers, by passwords, by network communication channels and encryption. In the health information system, ethical means of data protection is defined by IMIA (International Medical Informatics Association). Code of Ethics for medical and health informatics professionals must be clear, unambiguous and easily applicable in practice. Given that the IT field is in constant flux, the Code must be flexible to adjust to ongoing changes, without sacrificing the applicability of basic principles. The reason that the Code of Ethics for MHIPs is created instead of adjusting one of the codes designed for another group of IT professionals stands in the fact that MHIPs play a unique role in the planning and provision of health: a role which is distinct from that of other IT professionals working in different environments (International Medical Informatics Association, 2012).

With polyclinic activities, it is necessary to protect the doctor's reports, i.e. the data contained on it. Doctor's reports are protected in a way that each physician has his or her code or password, and can write or edit only their patients' reports, while they can only look at the others. Any physician can access the data in the database from any workstation or terminal. Administrators have far greater authority and rights. In certain application modules, administrators can access all the data and can provide or restrict authority or rights. Options

of a cardiologist in the observed information system (and the benefits) are as follows: (1) all the diagnostic laboratory reports are recorded in medical history or in a summarized discharge letter; (2) they have access to the previous reports of the same patient (archives); and (3) have Internet access (Inge and Mihalić, 2012). In the health information system, the data is protected by creating safety copy or back up daily. In the process of backing up, electronic data is stored on the server and three external storage media including: hard disk, DVD, and CD. To protect the electronic data effectively, anti-virus protection on the Internet is automatically updated. Since the patient data must not be lost in order to protect and secure the health information system, in addition to back up and anti-virus protection using firewall that filters communications packages and controls the traffic towards the local network and UPS (Uninterruptible Power Supply). UPS is an uninterruptible power supply system which is used in the health information system. The purpose of such a system is power supply of especially important information equipment with appropriate quality DC or AC voltage. It is widely known that the DC power systems are used to supply the most demanding consumers, which require an uninterrupted voltage, and in the case of power supply or additional aggregate supply failure.

When talking about the data integrity, in most departments only currently active physician can modify and print out their reports, while other reports can be only browsed. When one needs to print out a report, the printing can be done by the administrator. Administrator can print out any report.

In order to protect the health information system, it is necessary to ensure data confidentiality. Data confidentiality is ensured by passwords. In the health information system, it is strictly defined who is eligible to access a certain part of an electronic database, i.e. who has the authority to delete, create or update files and data stored in the file. Each physician must have a password to access a particular part of the application or a module. The password should be changed usually every month, and if necessary several times a month. An optimal password should be a minimum of seven characters. It is preferred for a password to contain a combination of uppercase and lowercase letters and numbers. It is by no means recommended to use first names, surnames, names of parents, children, date of birth, name of residence, street name, and the like for the password. It is not recommended to use for the password the same set of characters. Password change on the server or the application is done so that the user himself or herself changes the password. After the command for the password change is set, the user must first enter the current password, and after that the new password twice. In case the physician forgets the password, there is the administrator who will change it as needed. The password should not be written down on paper and put in a drawer in the office for security reasons and for the possibility that a third person comes to classified information about the patient.

When talking about a limited number of attempts to access the health computer system, the system must be adjusted to limit the number of possible accesses. If a user tries to access the health information system more than three times with a wrong password and username, the system must rejected them. The next desirable option to be set is the message of the last access to a particular part of the application or a particular module. The view of the last data access in the health information system should be provided in the form of dates, times, and names. Electronic data in the health information system can also be protected by locking the

passwords by the system administrator and by using stronger additional passwords or the dual password system.

Certain (reports) or the register in the health information system contain only numbers and never names (Inge and Mihalić, 2012).

The methods of preserving records in the health system – a case study

The owner of the data or databases in the health information system is the patient and his data should not be lost in any case. The patients' data must be permanently stored and archived. When it comes to archiving in the health information system, reports and discharge letters are automatically archived. If necessary, the data can be transferred from the old discharge letter to the new one. The information on the methods and ways of preserving electronic records and documents in the health information system for a longer period of time was collected using a survey called digitizing documents in the analogue form and the protection of e-documents (Stančić, 2005). The survey was filled in by an employee who is a part of the health information system and has sufficient experience in working with the observed information system.

Collecting the data by using survey and interview has led to following conclusions: the observed organization which uses the health information system (1) does not store materials or documents in digital form, but (1.1) is planning to store the materials and documents in electronic form. Based on the appointed secondary question 1.1.1., (what types of material and documents are planned to be stored by the company), the given answer was that the organization keeps records of all cases. The plan for the preservation of electronic documents of the observed organization is in the initial stage of construction (1.1.2.), and it plans to store the materials inside the organization itself (1.1.3.). In the question about the strategy of storing the materials and documents in electronic form, the interviewed employee says that the strategy is in the process of construction (1.1.4.) and that the construction of strategy for the preservation of materials and documents in electronic form is made with the help of external experts (1.1.5.). The observed organization intends to store the materials and documents which will originally appear in electronic form and to digitize existing materials and documents.

The key criterion that the observed organization considers as the main criterion for the selection of materials and documents for preservation is the legal obligation of their preservation. The interviewed and surveyed employee did not know (want) to answer the question of how much financial resources the observed organization is planning to invest into the system for the preservation of materials and documents in electronic form (1.1.8.).

The observed organization stores in the electronic form case files such as the documents of construction and adding on of a specific hospital. The organization's general preservation policy is in the process of developing a general conservation policy which includes the preservation of materials or documents in electronic form. The observed organization has a prescribed practice for (1) the transfer of preserved records from outdated formats into new formats of records (i.e. reformatting); (2) the update of the media (i.e., the replacement of depleted media with the new); (3) migration of records to a new type of media; and (4) emulation of outdated working environments or operating systems and other applications.

The observed organization has policies and defined programs for the preservation of materials and documents in digital form for a longer period of time. However, the problem is in the slow realization and implementation of activities for implementing the plan.

When it comes to collaboration, the observed organization has never cooperated with other companies or institutions to develop programs for the preservation of electronic records and documents. The employee who answered the questions and who is also the beneficiary of the health information system considers all electronic materials kept by the observed organization records. The observed organization has not been conducting any special preparations for the preservation of electronic materials which are considered records. The observed organization has not yet identified a problem, an obstacle or a threat to the integrity of electronic materials that might arise from the methods and techniques used.

Public health supervision system

Basic requirements for the public health supervision system are accuracy, timeliness, operability, originality and standardized quality. Accuracy refers to the continuous control and automaticity. Timeliness means the timely response of the public health supervision system without delay. Operability refers to data availability and flexibility in the creation of information. The public health information system includes the data from places where they occurred, for example from electronic health record and not from a special reporting form. Standardized quality includes a uniform terminology and international compliance (Kern, 2012).

RESEARCH ANALYSIS OF THE APPLICATION OF PROCEDURES FOR THE PRESERVATION OF ELECTRONIC MATERIALS AND DOCUMENTS

The questionnaire used in this paper is partly taken from the paper by Hrvoje Stančić entitled "Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata" ("Theoretical model of stable authentication preservation of electronic information objects") in order to collect data on organizations that are related to the preservation of electronic materials and documents. This study used a questionnaire consisting of 33 key questions. Besides these questions, the questionnaire contains a number of secondary questions. Each participant was an employee of the organization and it was clear already at the beginning that participants will not be in the position to answer every question. Mostly, the questions have been answered, except the questions about finances, due to the information sensitivity and value.

Table 1: Research analysis of the application of procedures for the preservation of electronic materials and documents

Questions and secondary questions	Answers:						
	Organization 1	**Organization 2**	**Organization 3**	**Organization 4**	**Organization 5**	**Organization 6**	**Organization 7**
1. Does your organization preserve materials/documents in electronic form? (B)	No	Yes	Yes	Yes	Yes	Yes	Yes
1.1. Does your organization plan to preserve materials/documents permanently in electronic form?	Yes	-	Yes	Yes	Yes	Yes	Yes
1.1.1. What type of materials/documents do you plan to preserve?	Case files	-	All types of documents and materials which need to be preserved according to the Document Archiving Act.	All types of documents and materials which need to be preserved according to the Document Archiving Act and all other documents, order form, offer, book of products, concluded contracts, financial reports, etc.	Travel warrants, the decision on establishing the organization, statute, application letter	All types of documents and materials which need to be preserved according to the Document Archiving Act and all other documents. Register book, register, travel warrants, degrees and certificates on teacher training, i.e. file, files on school construction, attests, testing, services, school statutes, registries and files, contracts, formal decisions on weekly and yearly schedule of teacher's work obligations, decisions on setting up or breaking up working contracts, applications and notices of cancellation, etc.	All types of documents and materials which need to be preserved according to the Document Archiving Act and all other documents. Register book, register, travel warrants, degrees and certificates on teacher training, i.e. file, files on school construction, attests, testing, services, school statutes, registries and files, contracts, formal decisions on weekly and yearly schedule of teacher's work obligations, decisions on setting up or breaking up working contracts, applications and notices of cancellation, etc.
1.1.2. In which phase is the creation of the plan for the preservation of electronic documents?	In the beginning	-	In process.	We do not make plans for the preservation but we realize the preservation of documents in electronic	In the beginning phase since the organization is quite young.	We do not make plans for the preservation but we realize the preservation of documents in electronic	We do not make plans for the preservation but we realize the preservation of documents in electronic

Questions and secondary questions	Answers: Organization 1	Organization 2	Organization 3	Organization 4	Organization 5	Organization 6	Organization 7
				form immediately.		form immediately.	form immediately.
1.1.3. Do you plan to keep materials/documents?	Inside the institution	-	Inside the institution	Of course, always.	Inside the institution	Inside the institution	Inside the institution
1.1.4. Do you have a developed strategy of preservation of materials/documents in electronic form inside your organization?	In construction	-	Yes, we do.	Yes, we do. You could say so.	In construction	Yes, we do. You could say so.	Yes, we do. You could say so.
1.1.5. The strategy of preservation of materials/documents in electronic forms has been/is being made:	Business secret	-	By ourselves inside the organization.	By ourselves inside the organization.	By ourselves inside the organization	By ourselves inside the organization.	By ourselves inside the organization.
1.1.6. Do you intend to keep materials/documents which are going to be originally created in electronic form?	Yes	-	Yes	Yes	Yes	Yes	Yes
1.1.7. Do you intend to digitize existing materials/documents?	Yes	-	Yes	Yes	Yes	Yes	Yes
1.1.7.1. Which of the following criteria will your organization consider main when choosing materials/documents for preservation?	Legal obligation of preservation	-	Legal obligation of preservation, saving space required for storage.	Legal obligation of preservation, saving space required for storage, historical, slow physical deterioration, improving access, commercial use of our own materials.	Historical / cultural importance, legal obligation of preservation, improving access, saving space required for storage.	Historical / cultural importance, legal obligation of preservation, improving access, saving space required for storage.	Historical / cultural importance, legal obligation of preservation, improving access, saving space required for storage.
1.1.8. What amount of finance resources is planned to be invested into the system for the preservation of materials/documents in electronic form?	Business secret (I do not know)	-	-	For now, it still cannot be estimated.	14000, 00 kuna	-	-
2. Describe which electronic material your organization preserves?	Case files and all the necessary documentation	CD	Disc, CD, microfilm.	All the documentation coming from the environment into our system and which goes out of the system into the environment.	More or less, all the material of the organization (order forms, maintenance plan, statute, members list, etc.)	Students lists with their personal data, their grades, contracts, registries, and all the documentation coming from the environment into our system in electronic form and which goes out of the system into the environment.	Students lists with their personal data, their grades, contracts, registries, and all the documentation coming from the environment into our system in electronic form and which goes out of the system into the environment.
3. Does your organization have a general preservation policy which includes the preservation of materials / documents in electronic	In the process of development	In the process of development	Yes. Preservation = obligational archiving according to	Yes. More or less all the documents coming into the company	In the process of development	In the process of development	In the process of development

Questions and	secondary questions	Answers: Organization 1	Organization 2	Organization 3	Organization 4	Organization 5	Organization 6	Organization 7
form?				the law.	and going out of it are stored in digital form and are preserved.			
4. Does your organization have a policy or prescribed practice for:	a) changing preserved records from outdated formats into new records (reformatting)	Yes	Yes	No	Policy? Yes	Yes	Yes	Yes
	b) refreshing the media (changing old media with new ones of the same type)	Yes	Yes	No	Policy? Yes	Yes	Yes	Yes
	c) migration of records on the new media type	Yes	Yes	Yes	Policy? Yes	Yes	Yes	Yes
	d) emulation of outdated work environments (operating systems and application)	Yes	Yes	No	Policy? Yes	Yes	Yes	Yes
	e) policy/ practice is in the process of development	In the process of development	I do not know	-	Policy is always in the process of development in that area	In the process of development	In the process of development	In the process of development
	f) something else	X	I do not know	-	-	X	-	-
5. Does your organization have a defined program or policy for the preservation of materials/documents in electronic form for a longer time period?		Yes	Yes	Yes	It is not clearly defined; however, the preservation of materials and documents is performed in electronic form.	No	No	No
5.1. In which year did the program/activity of preserving materials in electronic form start?		I do not know	1990	1995	From the beginning of digitalization of documents in the company.	2011	I do not know	I do not know

Questions and secondary questions	Answers:						
	Organization 1	Organization 2	Organization 3	Organization 4	Organization 5	Organization 6	Organization 7
				More precisely, from the time of the company establishment			
5.2. Is there any problem which influences the implementation of the program and activities?	Yes, slow implementation.	No	No	No	No	No	No
6. Do you use certain methods and/or techniques with the purpose of preserving materials in electronic form?	No	Yes	No	Yes	Yes	Yes	Yes
6.1. Generally describe the methods and/or techniques used for the preservation of materials in electronic form.	-	Materials which can be found on the server are protected against viruses, and materials are stored on several storage media.	-	Migration; changing file formats from one into another, depending primarily on the change of operating system and application program.	Photographing and scanning of the documents	Photographing and scanning of the documents and changing file formats from one into another. .XLS format into .XML format (program code).	Photographing and scanning of the documents, and changing file formats from one into another. XLS format into .XML format (program code).
6.2. If you do not preserve materials in electronic form, do you study/estimate certain methods and/or techniques as those which you might use in future?	Yes	No	No	We perform it	-	-	-
7. Have the other organizations or individuals collaborated (or collaborate or you plan collaboration) with your institution on the development of the preservation program?	Yes	No	Yes	No	No	No	No
7.1. Those were/are/will be:	All those who have experience in preserving electronic documents, graduated IT professionals, and other ICT experts.	-	Specialized agency	-	-	-	-
7.2. Is your collaboration (was/will be):	-	-	Of local character	.	-	Of local character	Of local character
8. Do you have some special preparations for the preservation of electronic materials you consider records (as different from the preservation of other electronic materials)?	Yes	Yes	No	Yes	Yes	No	No
8.1. If yes, please state which.	Preparing the medium for storage, and preparing appropriate input and output units.	Preparing the medium for storage (CD, USB)	-	Preparing the medium for storage (CD, DVD, USB memory, preparing the discs (internal and	Switching the records from the specific file on one storage medium to other data storage	-	-

Questions and secondary questions	Answers: Organization 1	Organization 2	Organization 3	Organization 4	Organization 5	Organization 6	Organization 7
				external)).	medium.		
9. Has the program and/or the activity come to the point of testing or evaluation of any of the methods or techniques which you use?	No	No	No	No	Yes	-	-
9.1. If yes, what are the results/conclusions?	No	-	-	-	Good (Without a specific explanation)	-	-
9.2. Have you identified any problems, obstacles or threats for the integrity of electronic materials which would appear due to used methods or techniques?	No	-	No	-	No	No	No
10. Which of the following criteria are main criteria when choosing materials for the preservation? (C)	Legal obligation of preservation	Legal obligation of preservation and access improvement	-	Legal obligation of preservation and access improvement, and documentation which is necessary in future for tenders, i.e. the need for specific documents, etc.	Access improvement	Eased data access (availability)	Eased data access (availability)
11. Where do the materials you keep come from?	Mostly from the companies soliciting for tenders, and from governmental institutions.	From the parent body	-	From the parent body and from the environment.	From the parent body, and from other institutions (counties).	From the parent body, and from other institutions (counties, town, education and teacher training agency, etc.).	From the parent body, and from other institutions (counties, town, education and teacher training agency, etc.).
12. Which technique/method do you use for preservation? (D)	Archiving of all documents and storing the records of the archives on a CD. After a certain time, refreshing of the medium the important data is stored on is performed.	Storing the records of the archives on a CD.	-	Archiving of all documents and storing the records of the archives on a CD. After a certain time, refreshing of the medium the important data is stored on is performed.	Programming new software, i.e. improving the existing application, standardization of formats, migration, replication (records are copied without changes on the new generation media).	Standardization of formats, migration, replication (records are copied without changes on the new generation media).	Standardization of formats, migration, replication (records are copied without changes on the new generation media).
13. Which technique/method characteristics you use do you find good and why?	We consider it a good and useful solution to use the data registering program and JIT data finding for a certain case in	I do not know how to express myself.	-	-	The feature of preserving the object in its original form. Replication.	-	-

Questions and	secondary questions	Answers:						
		Organization 1	**Organization 2**	**Organization 3**	**Organization 4**	**Organization 5**	**Organization 6**	**Organization 7**
		a very short period of time, and finding out which department certain case is in and at which official.						
14. Do you use the hybrid model, e.g. a combination of two or more techniques/methods, like microfilming, scanning, and photographing?		Yes	Yes	Yes	Yes	Yes	Yes	Yes
14.1. Which model is that and how was it developed?		Scanning and photographing and earlier in the past microfilming was used.	Scanning and photographing	Scanning and photographing and earlier in the past microfilming was used.	Photocopying, microfilming, scanning.	Scanning and photographing, and conversion of .pdf formats into .doc and .docx formats.	Scanning and photographing, and conversion of .pdf format into .doc and .docx formats and conversion from .xls format into .xml format.	Scanning and photographing, and conversion of .pdf format into .doc and .docx formats and conversion from .xls format into .xml format.
15. In what way is the method/technique your organization uses different from other methods/techniques you tried/used before or do you know whether the other institutions are using them?		Easier navigation, retrieval and faster access to specific data.	There is no difference.	-	We did not use any other possibilities of preserving the records	We did not use any other possibilities of preserving the records	We did not use any other possibilities of preserving the records	We did not use any other possibilities of preserving the records
16. Have you taken into consideration possible impacts for the intellectual integrity (e.g. authenticity) of preserved materials when choosing the method/technique/strategy for preservation?		No	No	Yes	No	No	No	No
17. If you keep e-documents and materials, please state the record formats in question, according to the type of the preserved material (text, picture, video, web pages, etc.).		Text – .pdf, .doc, .docx, .odt Picture- .jpg, .jpeg. Sound- we do not preserve. Video- we do not preserve. Web pages- .hmtl, .css	Text – .txt, .pdf, .doc, .docx. Picture- .jpg, .jpeg. Sound- we do not preserve. Video- we do not preserve. Web pages- .hmtl, .css.	Text – .txt, .pdf, .doc, .docx. Picture- .jpg, .jpeg. Sound- we do not preserve. Video- we do not preserve. Web pages- .hmtl, .css.	Text – .txt, .pdf, .doc, .docx. Picture- .jpg, .jpeg. Sound- midi, mp3, mp4, wav, wave, cda, swa, voc. Video-avi. Web pages- .hmtl, .css. Bitmap (BMP), TIFF, GIF, HTML, FlashPix (FPX), TIFF compressed, DCX, PCX, RTF, CRV, PNG Mac: PICT, TIFF, JPEG, TIFF compressed, GIF, TEXT, HTML,	Text – .pdf, .doc, .docx, .odt Picture- .jpg, .jpeg. Sound- we do not preserve. Video- we do not preserve. Web pages- .hmtl, .css	Text – .pdf, .doc, .docx, .odt Picture- .jpg, .jpeg. Sound- we do not preserve. Video- we do not preserve. Web pages- .hmtl, .css Databases are preserved in .mdb format, .accdb format and .xml format.	Text – .pdf, .doc, .docx, .odt Picture- .jpg, .jpeg. Sound- we do not preserve. Video- we do not preserve. Web pages- .hmtl, .css Databases are preserved in .mdb format, .accdb format and .xml format.

Questions and secondary questions	Answers:						
	Organization 1	Organization 2	Organization 3	Organization 4	Organization 5	Organization 6	Organization 7
				FlashPix (FPX)			
18. Do you digitize materials?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
18.1. If you digitize, which devices do you use for that purpose?	Scanner and camera	Scanner and camera	Scanner and camera	Scanner, camera and video camera.	Scanner and camera	Scanner and camera	Scanner and camera
18.2. Which programs do you use?	Different programs, usually those that come in a package with the devices themselves (input units).	Different programs, usually those that come in a package with the devices themselves.	Different programs, usually those that come in a package with the devices themselves.	HP Photo & Imaging Software, NewSoft Presto! BizCard, Adobe Photoshop Elements, IRIS ReadIris Pro, Adobe Acrobat Reader.	HP Photo & Imaging Software, Adobe Acrobat Reader.	HP Photo & Imaging Software, NewSoft Presto! BizCard, Adobe Photoshop Elements, IRIS ReadIris Pro, Adobe Acrobat Reader.	HP Photo & Imaging Software, NewSoft Presto! BizCard, Adobe Photoshop Elements, IRIS ReadIris Pro, Adobe Acrobat Reader.
18.3. Which record format do you use when digitizing?	.pdf, .jpg, .jpeg, .gif, tools for the conversion of .pdf format into .docx format.	.pdf, .jpg, .jpeg, .gif, .doc, .docx.	.pdf, .jpg, .jpeg, .gif, tools for the conversion of .pdf format into .doc and .docx formats.	.pdf, .jpg, .jpeg, .gif, tools for the conversion of .pdf format into .doc and .docx formats.	.pdf for business documents. .jpg and .jpeg for pictures and photographs	.pdf, .jpg, .jpeg, .gif, .doc, .docx, .xls, .xml	.pdf, .jpg, .jpeg, .gif, .doc, .docx, .xls, .xml.
18.4. Which technical settings do you use when digitizing for the features like resolution and important pixel depth (color number) with picture materials, important sound depth with sound materials, etc.?	Settings that provide maximum image size to 6MB to avoid e-material taking too much memory space, i.e. data storage medium.	Default settings	Recommended settings.	Recommended settings.	-	Recommended settings.	Recommended settings.
18.5. Do digitized materials go through the additional processing (e.g. optical character recognition (OCR), color adjustment, contrast adjustment, additional rotation, cropping, etc.)?	They go through minimum processing to make e-records seem as authentic as possible.	No	No	Yes	No	Yes	Yes
18.6. Do you compress digitized materials?	Sometimes (very rarely).	Yes	Yes	Yes	No	Yes	Yes
18.6.1. If you compress, which is/are the format/s of compressed record you use?	.zip, .rar	.jpeg, and .zip and .rar.	.zip, .rar	.zip, .rar	-	.zip, .rar or the same format in compressed form .bmp	.zip, .rar or the same format in compressed form .bmp
18.6.2. Do you keep the original, uncompressed copy?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
19. Are the preserved materials described according to accepted standards?	Yes	No	Yes	Yes	No	Yes	Yes
20. Which methods of quality control do you use in the process of preserving electronic records? (E)	Own methods such as control of the time when the data was recorded on a specific data	I do not know.	-	Own methods such as control of the time when the data was recorded on a specific data	-	-	-

Questions and secondary questions	Answers:						
	Organization 1	Organization 2	Organization 3	Organization 4	Organization 5	Organization 6	Organization 7
	storage medium.			storage medium.			
21. How and where (physical location) do you store preserved electronic records?	In the archive. Electronic records are in the e-archive and on the record storage media according to the case code and name.	In the locked archive.	In the same building.	In the archive. Electronic records are in the e-archive and on the record storage media according to the case code and name.	In a room in our organization	In a room in our organization	In a room in our organization
22. On which media do you store preserved records?	CD-R, DVD-R, CD-RW, DVD-RW.	CD, USB.	Microfilm, CD-R, DVD-R, CD-RW, DVD-RW, USB.	Microfilm, CD-R, DVD-R, CD-RW, DVD-RW, USB.	On internal hard disc, DVD, CD, on external hard disc. The media is stored in locked drawers which are immovable in special locked rooms.	On internal hard disc, DVD, CD, CD-RW, DVD-RW, USB and on external hard disc. The media is stored in locked drawers which are immovable in special locked rooms.	On internal hard disc, DVD, CD, CD-RW, DVD-RW, USB and on external hard disc. The media is stored in locked drawers which are immovable in special locked rooms.
23. Do you make back-up copies?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
23.1. How many copies do you make and how often?	I do not want to give this information.	Two copies, once a year.	-	The data is stored on a new disc every 3 days. Once every three days.	Once every two weeks a back-up is created, i.e. twice a month.	A copy is created every day, but for certain data only.	A copy is created every day, but for certain data only.
23.2. Where do you store them (physical location in relation to the placement of the original data)?	I do not want to give this information.	In the same building.	In the same building	In the same building	In the same building	In the same building	In the same building
24. Is there any kind of access constraint to the preserved records? (G)	There is a physical access constraint to the data which is on the media such as CD or DVD. It is not possible to access the server with important e-data without the password.	No	-	There is a physical access constraint to the data which is on the media such as CD or DVD. It is not possible to access the server with important e-data without the password.	Yes	Yes	Yes
25. Is the system the preserved records are in equipped by mechanisms for the access control?	The system is not equipped with special mechanisms for the access control; however, it can be determined who accessed the server	No	-	Yes	Yes	No	No

Questions and secondary questions	Answers: Organization 1	Organization 2	Organization 3	Organization 4	Organization 5	Organization 6	Organization 7
	when or who accessed the archive space where the media with stored e-data are.						
26. Are the preserved records available?	Only inside the institution	Strictly where they are preserved.	-	Strictly where they are preserved, only inside the institution, via specific software module.	The preserved records are available strictly where they are preserved and only inside the organization.	The preserved records are available strictly where they are preserved and only inside the organization.	The preserved records are available strictly where they are preserved and only inside the organization.
27. Is the system the preserved records are in connected to:	The server which is in the institution.	The server which is in the institution.	-	The server which is in the organization, intranet.	The server which is in the institution.	The server which is in the institution.	The server which is in the institution.
28. Is there a possibility of searching preserved records in the system?	Yes	No	-	Yes	Yes	Yes	Yes
29. Which categories can they be searched in?	Class, name, year, date, size, employee.	-	-	Class, name, year, date, file size, employee who created the document.	File size, date and file name.	File size, date and file name.	File size, date and file name.
30. Do you keep copyright materials in electronic form? (H)	No	No	-	No	No	No	No
30.1. Does your organization have copyrights for electronic form of the record?	No	-	No	No	Yes	For some records yes, and some no.	For some records yes, and some no.
30.2. Are the users allowed to perform any of the mentioned activities related to the preserved materials?	Printing	They are not allowed to do any of it	-	Printing, transferring materials on personal computer, transferring materials on local network.	Printing, transferring materials on personal computer, transferring materials on local network.	Printing, transferring materials on personal computer, transferring materials on local network.	Printing, transferring materials on personal computer, transferring materials on local network.
30.3. Does your organization use a system for electronic management for the control/ supervision/registering of creating copies?	Yes	No	Yes	Yes	No	No	No
31. In your estimation, what are the expenses of preserving records?	Business secret (I do not know)	Business secret (I do not know)	-	Business secret (I do not know)	I cannot estimate, minimum.	I cannot estimate; we try to make them minimum.	I cannot estimate; we try to make them minimum.
32. Please describe the categories of expenses for the preservation of records, id they exist (personnel, equipment, hardware, software, storage media, space and energy used, etc.)	Business secret (I do not know)	Business secret (I do not know)	-	Business secret (I do not know)	The expenses for the preservation of records are the storage space and energy used.	The expenses for the preservation of records are made by the storage space and energy used.	The expenses for the preservation of records are made by the storage space and energy used.
33. Which resources is the process of preservation funded from and how are they distributed?	Business secret (I do not know)	Business secret (I do not know)	-	Business secret (I do not know)	Business secret	-	-

Source: Created by the authors of the paper on the basis of data collected by questionnaire from the employees of relevant organizations and by the questionnaire from the paper by Stančić Hrvoje "Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata" ("Theoretical model of stable authentication preservation of electronic information objects"). Doctoral dissertation. Survey. Zagreb 2005.URL: http://bib.irb.hr/datoteka/244465.Ocuvanje_autenticnosti_e-informacijskih_objekata.pdf

On the basis of the table 1, we can see and compare the methods for the preservation of documents and materials, electronic documents and electronic materials which are used by the observed and surveyed organizations. Surveyed organizations are state-owned, privately owned and owned by the municipalities and towns. Employees who were surveyed have a university degree in economics (organization 1, 2 and 4), and in Information Technology (organizations 3, 5, 6, 7). The only problem that was present during the survey was finding experts in these organizations who have experience in long-term preservation of electronic materials and documents. Organization 1 is a part of the executive power in the Republic of Croatia, where the research was conducted. Organization 2 is a private company which specializes in import and distribution of fertilizers, agricultural products and feed additives. Organization 3 is an IT company for software development and troubleshooting of hardware for all types of computers. Organization 4 is a public organization owned by the municipalities and towns whose main activity is natural gas supply and distribution in a certain county. Organization 5 is an association which operates and performs activities in the field of finance and information technology for a longer period of time. Organizations 6 and 7 are educational organizations. On the basis of Table 1, the results of the research can be seen and it can be concluded that most organizations use a scanner and a camera to digitize documents; mostly, the digitized documents and electronic records are stored in .pdf, .doc, .docx, and .xml formats. When the safety of digitized documents and the possibility of the documents to be opened by malicious people is taken into account, it is best to store the digitized document in .odt format since the tools for opening documents and records in that format are less frequently used. The data collected from field studies indicate that representatives of the organizations that provided the data do not want to give in public the information on the amount of financial resources they would invest in the preservation of electronic materials and documents. The release of information from the plan of investing financial resources in the future is clearly not pleasant these days. Based on Table 1, the results of the company, i.e. observed organization, can easily be compared.

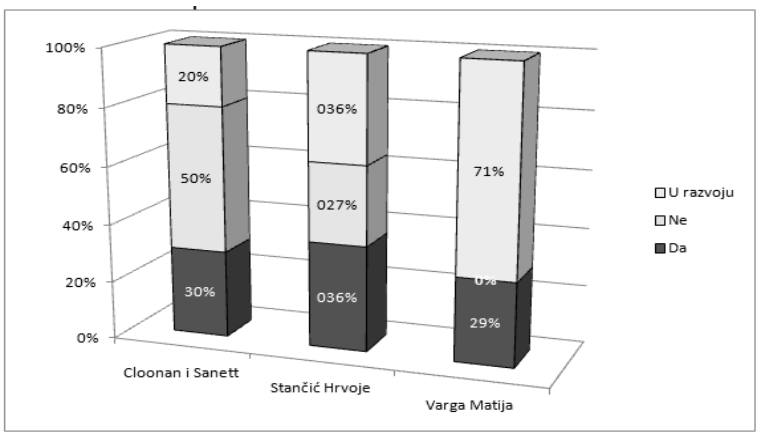

Figure 1: Does the institution have a general policy of preservation which includes the preservation of materials in electronic form?
Source: Created by the authors of the paper in MS Excel and on the basis of data collected by questionnaire from the employees of the observed organizations and the questionnaire created on the basis of the questionnaire from the paper by Stančić Hrvoje "Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata" ("Theoretical model of stable authentication preservation of electronic information objects"). Doctoral dissertation. Survey. Zagreb 2005. URL: http://bib.irb.hr/datoteka/244465.Ocuvanje_autenticnosti_e-informacijskih_objekata.pdf. Legend: In the process of development (U razvoju); No (Ne); Yes (Da); Cloonan and Sanett (Cloonan i Sanett)

Figure 1 indicates general preservation policy which includes the preservation of materials in electronic form. It is necessary to take into account that the time gap between the surveyed organizations and the conducted research between the first and the second case is five years, while the interval between the second and the last research presented in the first figure is 7 years. In the first case, in the figure 1, foreign institutions are the subject, while the other two figures show the results of local institutions or organizations. The research which was conducted over a period of one month and with a sample of 7 organizations, it is shown that there is no organization that has no general record and material preservation policy in electronic form.

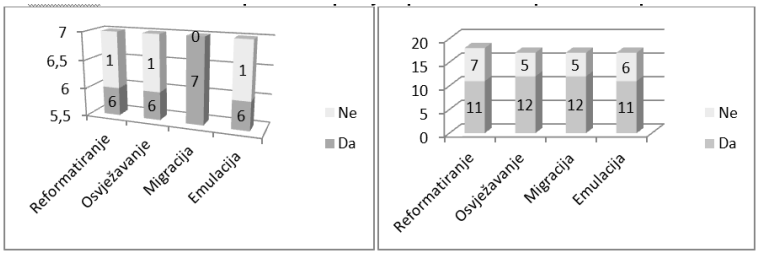

Figure 2: The existence of prescribed policy or practice for the preservation procedures
Source: Created by the authors of the paper in MS Excel and on the basis of data collected by questionnaire from the employees of the observed organizations and the questionnaire created on the basis of the questionnaire from the paper by Stančić Hrvoje "Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata" ("Theoretical model of stable authentication preservation of electronic information objects"). Doctoral dissertation. Survey. Zagreb 2005. URL: http://bib.irb.hr/datoteka/244465.Ocuvanje_autenticnosti_e-informacijskih_objekata.pdf
Legend: Reformatting (Reformatiranje); Refreshing (Osvježavanje); Migration (Migracija); Emulation (Emulacija); No (Ne); Yes (Da).

Figures 2 show the results of processing data collected on the basis of a questionnaire. We examined the existence of a policy or prescribed practice for switching the preserved records from outdated record formats into new ones (reformatting); refreshing the media (the replacement of depleted media with the new ones of the same type); migration of the records to the new media type; and emulation of outdated working environments (operating systems/programs). Of the seven surveyed institutions, seven of them responded to this question. All organizations are performing the migration process, which is shown in the left figure. If the collected research data from the research in the paper by Hrvoje Stančić and the research that took place in 2012 were combined, the size of the sample would increase to 18 organizations, and obtained results would be different (figure 2).

Table 2: The comparison of collaboration of organizations with other organizations

Type of collaboration	Cloonan and Sanett	Hrvoje Stančić	Matija Varga
International	11	3	0
On national level	10	4	0
Of local character	2	2	3
Of institutional type	0	5	0
Using the common space/equipment	1	0	0

Source: Created by the authors of the paper in MS Word and on the basis of data collected by questionnaire from the employees of the observed organizations and the questionnaire created on the basis of the questionnaire from the paper by Stančić Hrvoje "Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata" ("Theoretical model of stable authentication preservation of electronic information objects"). Doctoral dissertation. Survey. Zagreb 2005.(Modified)

Table 2 presents the comparison of results of three studies and shows the collaboration of the organizations with other organizations in the development of the preservation program. A five-year gap is between the first and the second research, and a seven-year gap between the second and the third research of the collaboration in the development of the preservation program. Based on the latest research, the most common form of collaboration in the observed organizations is of local character. Most of the observed organizations did not answer the question about collaboration between organizations, and three organizations have (will have) the collaboration of local character.

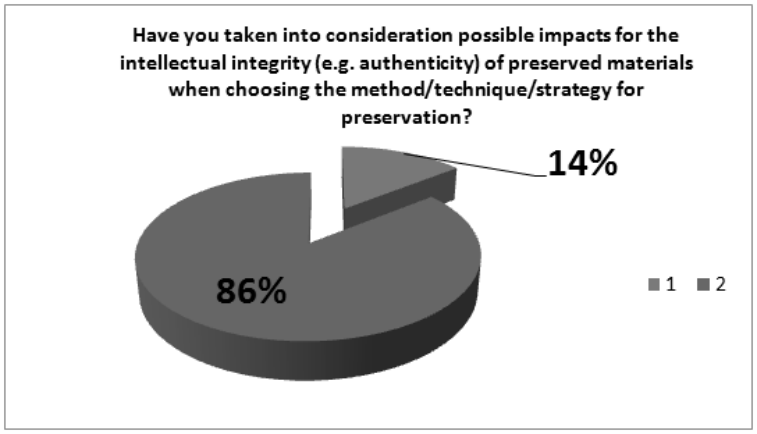

Figure 3: The influence on the intellectual integrity (e.g. authenticity) of the preserved electronic materials.

Source: Created by the authors of the paper in MS Word and on the basis of data collected by questionnaire from the employees of the observed organizations and the questionnaire created on the basis of the questionnaire from the paper by Stančić Hrvoje "Teorijski model postojanog očuvanja autentičnosti elektroničkih informacijskih objekata" ("Theoretical model of stable authentication preservation of electronic information objects"). Doctoral dissertation. Survey. Zagreb 2005. (Modified).

Figure 3 presents whether the organizations or employees, when selecting methods/techniques/strategies for preservation, have taken into account the possible impacts on intellectual integrity (authenticity) of preserved electronic materials. The question "Have you taken into consideration possible impacts for the intellectual integrity (e.g. authenticity) of preserved materials when choosing the method/technique/strategy for preservation?" the participants answered once with *yes* and six times with *no*.

CONCLUSION

The paper explains the reason for creating a Code of Ethics for Medical Health IT professionals. Based on the information collected by the questionnaire, it can be concluded that organizations mostly use cameras and scanners to digitize documents, and that the digitized document is usually stored in .pdf, .doc .docx and xml format. When the safety of digitized documents and the possibility of the documents to be opened by malicious people is taken into account, it is best to store the digitized document in .odt format since the tools for opening documents and records in that format, as well as the Linux operating system that supports Open Office, are less frequently used. The data collected from field studies indicate that representatives of the organizations that provided the data do not want to give in public the information on the amount of financial resources they would invest in the preservation of electronic materials and documents.

The results of the research, which was conducted during the period of three weeks in 2012 on the sample of seven organizations, show that there is no organization that does not have a general policy of preserving the material in electronic form. The recommendation for the observed organizations is to back up electronic databases more often, or as many times as possible in the shortest period of time possible. The research presented in this paper, when it comes to collaboration in the development of the programs intended for preservation, shows that the most common form of collaboration is of local character. Organizations, when selecting methods, techniques and strategies for the preservation of the records do not take into account possible impacts on intellectual integrity (e.g. authenticity) of preserved electronic materials (86% of the total number of surveyed representatives of the organizations), which is worrying or the participants did not understand the question well enough.

REFERENCES

1. Bonić, M. (2011), Bez IT sustava nije moguće poslovati, Poslovni dnevnik, Moja ulaganja, Dnevnik d.o.o., Zagreb.
2. Inge, H., and Mihalić, G. (2012), Informacijski sustav u poliklinici za prevenciju kardiovaskularnih bolesti i rehabilitaciju, Materijali s predavanja, Menadžment u zdravstvu, MEF.
3. Kern, J. (2012), Zdravstveni informacijski sustav – pojam i značenja, Materijali s predavanja, Menadžment u zdravstvu, MEF.
4. Lee, M., and Gentry, B. (2005), Microsoft SQL Server 2008, Kompjuter biblioteka.
5. Stančić, H. (2005), Teorijski model postojanja očuvanja autentičnosti elektroničkih informacijskih objekata, Doktorska disertacija, Anketa, URL:

http://bib.irb.hr/datoteka/244465.Ocuvanje_autenticnosti_einformacijskih_objekata.pdf. Zagreb.

6. Varga, M., Ćurko, K., Panian, Ž., Čerić, V., Vukšić, B. V., Srića, V., Požgaj, Ž., Strugar, I., Spremić, M., Pejić Bach, M., Vlahović, N., Jaković, B. (2007), Informatika u poslovanju, Sveučilište u Zagrebu, Zagreb.
7. "International Medical Informatics Association", URL: http://www.imia-medinfo.org/new2/ pubdocs/Craotian_Translation.pdf (accessed 18 March 2012).