УДК 004.056.5:614.38

CYBERSECURITY IN THE EXCHANGE OF BIOMETRIC AND BIOMEDICAL DATA

КІБЕРБЕЗПЕКА В ОБМІНІ БІОМЕТРИЧНІ ТА БІОМЕДИЧНІ ДАНІ

Hristov H.A.[1], Batalov F.I.[2]
Христов Х.А.[1], Баталов Ф.І.[2]

[1, 2,] Technical faculti SWU"Neofit Rilski"-Blagoevgrad (Bulgaria)
ORCID: [1] https://orcid.org/0009-0002-0714-7614 , [2] https://orcid.org/0000-0001-7328-1526
E-mail: [1]hristo.a.hristov.66@gmale.com, [2]batalov@swu.bg

DOI: 10.15673/atbp.v16i3.2924

Abstract.. *Demographic change, such as the rapidly aging populations in many industrialized countries, along with the rise in chronic diseases (such as diabetes and heart disease), has prompted many professionals to explore how technology can alleviate the burden on healthcare workers and provide effective tools for the elderly. In particular, IoT (Internet of Things) technologies can play a key role in helping individuals manage their health issues at home. This has led to the development of "personal health devices" that allow individuals to monitor their health condition at home and share this data with healthcare providers and caregivers.*

The integration of "cloud" technologies into medical services is crucial for the large-scale deployment of reliable, high-tech solutions aimed at enabling self-monitoring for a broad user base. However, as modern information and communication technologies become increasingly embedded in healthcare, one of the most critical factors remains the reliability and security of medical, biomedical, and biometric data. From this perspective, ensuring cybersecurity in the deployment of such systems and services is of paramount importance.

Анотація. *Демографічні зміни, зокрема швидке старіння населення у багатьох промислово розвинених країнах, а також зростання хронічних захворювань (таких як діабет і хвороби серця), спонукають багатьох фахівців досліджувати, як технології можуть допомогти зменшити навантаження на медичних працівників і забезпечити корисні інструменти для людей похилого віку. Особливо важливим є те, як технології Інтернету речей (IoT) можуть допомогти людям вирішувати проблеми зі здоров'ям у домашніх умовах. Це призвело до розвитку "персональних медичних пристроїв", які дозволяють людям контролювати стан свого здоров'я вдома та передавати цю інформацію медичним працівникам і доглядачам.*

Використання "хмарних" технологій у медичній сфері має велике значення для масового впровадження надійних, високотехнологічних рішень, що забезпечують самоконтроль для широкого кола користувачів. Проте, з огляду на поширення сучасних інформаційних та комунікаційних технологій у сфері охорони здоров'я, одним із найважливіших аспектів залишається надійність і захист медичних, біомедичних та біометричних даних. З цієї точки зору, забезпечення кібербезпеки під час впровадження таких систем і сервісів є надзвичайно важливим.

Keywords: cybersecurity, information technology,biometric and biomedical data, "cloud" technologies
Ключові слова: кібербезпека, інформаційні технології, біометричні та біомедичні дані, "хмарні" технології

I. INTRODUCTION

In recent years, the topic of data protection in all public sectors has prevailed and become an emphasis in the policies of each country. Healthcare, in addition to being one of the largest and most complex socio-economic sectors in any country, requires a systematic and targeted approach to data and process management so as to successfully address the challenges in the field.

A trend in the development of modern healthcare is the transition to an entirely new model, the so-called 4P medicine based on four main principles: personalization, predictability, prevention and participation. The focus of 4P medicine is on the individual approach to the patient in order to early preclinical detection of diseases and the development of a complex of preventive measures - which means that doctors will regularly start prescribing not only certain drugs, but also software applications and mobile wearable devices collecting data on the physiology of the patient.

The use of digital medical devices opens up new opportunities for both biomedical research and clinical practice[13]. The need for the use of digital solutions in the sector and guarantees for security and process control is growing. The rapid pace of technology development leads to progress in this area, but also creates prerequisites for more cyberattacks, the damage of which can have serious consequences for any health structure.

In today's society - biometrics and biometrics in general are widely used in every field, best fitting into identification and security. The word biometrics comes from the Greek words life (Bios) and measurement (Metron). "Biometrics are an automated method of recognizing and identifying a person based on their physical or behavioral data or the given physical or behavioral characteristics of the body." Biometrics are physically measurable samples that are used to recognize an "object," and this can help fit into society as an important method of recognizing and identifying people. A biometric system is an automated system that can register individual biometric templates, extract biometric data from them, compare them with other biometric data, and finally tell us whether the identification process is successful or not. Although the technology itself is really new, since ancient times different peoples have used biometrics for recognition and identification. In Babylon, China, Japan, Assyria, etc., fingerprints were used in commercial transactions, marriage, and other contracts. The first attempt at a biometric relatively new identification system was set up by Edward. R. Henry and Francis Gilton in 1876. and includes a fingerprint identification method, and the method itself is called "dactyloscopy"[1]

II. LITERATURE ANALYSIS

Current trends in eHealth indisputably indicate that the exchange and management of clinical data should be based on internationally recognized standards and technical specifications in medical informatics. These standards and specifications must underpin the establishment of any healthcare infrastructure and information system.

On the one hand, this helps to build a unified information model for the exchange of clinical data between many different sources of such data, on the other hand it is significantly different from the information models used in the general case for modeling data exchange in informatics.

One of the significant differences is that information models based on standards in medical informatics are built in accordance with the typical business processes in medicine for the creation and use of clinical data for the treatment of patients. Most often, clinical data are presented in electronic format as a record in which all necessary information for the treatment and monitoring of the patient is stored. Such information, in particular, is disease history, immunizations, allergies, drug prescriptions and specialized patient examinations [2].

2.1. Security in IoT

Modern biometric and biomedical devices are a subclass in a larger class of devices – called Internet of Things devices. The Internet of Things can be seen as a vast network of connected microdevices, sensors, and small computers generating vast amounts of data it's all around us. In fact, it's hard to find an industry that remains untouched by IoT.

Azure IoT is Microsoft's cloud platform providing infrastructure and tools that facilitate the deployment, management, and retrieval of useful information from IoT devices. Azure IoT Suite is a complete solution with built-in security tools that provide protection at every level. At Microsoft, software security is an integral part of the development process, in line with decades-old principles for designing reliable and secure software. To this end, the Secure Application Development (SDL) lifecycle, a basic software development methodology combined with a set of Operational Security Assurance (OSA) services, as well as the Microsoft Digital Crimes Unit, Microsoft Security Response Center, and Microsoft Malware Protection Center, are used. Azure IoT Suite offers unique features that make it simple, visual, and most importantly, secure for providing, connecting, and storing data from IoT devices, providing strong security, privacy, and compliance. [3]

The security of the IoT infrastructure depends on the integrity of the code executed on each device individually. This code is used to authenticate the device and users, identify device ownership (and the data it generates), and protect against network and physical attacks by attackers. Microsoft Azure IoT Suite includes built-in security and privacy components on the Azure platform, as well as SDL and OSA processes, all of which are used to securely develop and work with Microsoft software.

These procedures provide infrastructure and network protection, as well as identity and management functions that are key to the security of any solution. One new Microsoft development is the Azure IoT Connector for FHIR, an API feature that allows healthcare organizations to scale secure connections for a large number of devices that transmit secure health information. As health systems increase the use of telemedicine and especially remote monitoring systems for patients, they are looking for technology to help them manage many connected devices at once, allowing them to improve the delivery of care in patients' homes.

The Azure IoT Connector for FHIR uses the HL7 Fast Healthcare Interoperability Resources specification to ensure secure and interoperability between medical devices and electronic health records when transmitting data over the Internet.

Today, remote data collection often uses device-specific platforms, making it difficult to scale when new processes are added or patients use multiple devices. Developers need to build their own secure channels for exchanging data with such devices every time. An Azure IoT Connector diagram for FHIR, available as a feature in the Microsoft FHIR cloud service, is shown in (Fig.1), everything is simplified. It is now possible to quickly and easily establish secure communication with IoT (Internet of Things) devices. The connector can connect to device-to-cloud or cloud-to-cloud workflows. Health data can be uploaded to Event Hub, Azure IoT Hub, or Azure IoT Central and converted to FHIR resources, allowing clinicians to view patient data from IoT devices in the context of clinical records supporting FHIR.

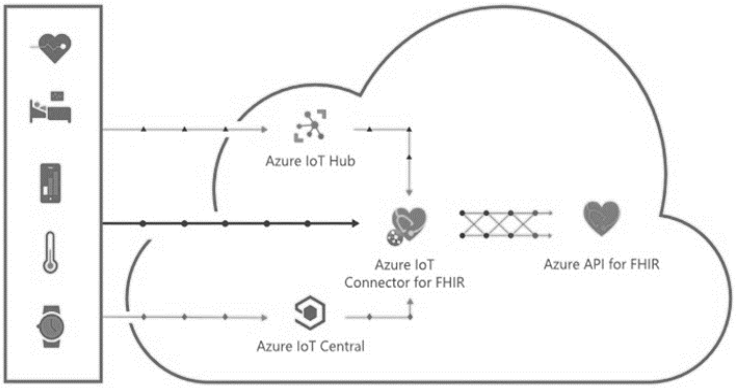

Fig. 1 Azure loT Connector for FHIR

Azure IoT Connector supports FHIR capabilities, such as:
- Converting biometrics from connected devices to FHIR resources;
- Scalability and real-time data processing;
- Integration with Azure IoT and Azure Stream analysis tools Role-based access control;
- Audit log tracking and security compliance array.

2.2. Modern IoT-based systems for the exchange of medical information to monitor the human condition.

Over the past 40 years, a large number of different standards for electronic medicine have been developed worldwide. Although in general there is no universal standard, and different standards are often applied in different aspects of such a huge field as medicine. The most common standards are Digital Imaging and Communications in Medicine (DICOM), Electronic Data Interchange for Administration, Commerce and Transport(EDIFACT), Open electronic health record (openEHR), xDT, Health Level Seven (HL7). As can be seen from (Table 1), the HL7 standard shows the best results in comparative functionality between them and is currently the most distributed.

One of the main challenges in medical informatics is the exchange, integration and processing of different types of information by data providers who use information models incompatible with each other. The level of efficiency and quality of health services, as well as the management of resources in the health system of each country, directly depends on finding a solution for the implementation of compatibility between these information systems.

There are different classifications of the level of compatibility between information systems. The lowest level (compatibility) between any two such systems can be achieved by adapting the syntactic means of presenting the data or the means of performing operations with the data. When the goal is to preserve the context of limitations and clinical conditions that accompany the data being exchanged, we are talking about semantic compatibility (interoperability). In this case, when transmitting the data, their correct interpretation is ensured, i.e. their semantic correspondence from a clinical point of view.

Unlike simple compatibility between two separate systems, interoperability is based on the application of established open standards for the presentation of data and clinical concepts.

Table 1 Comparison of the functionality of exchange standards Medical information

The name of function	**DICOM**	**xDT**	**EDIFACT**	**HL7/CDA**
Hospital Information System	X	X	X	X
Radiology Information	X	–	–	X
Image storage and sharing system	X	–	–	X
The main index of patients	–	X	–	X
Graphical diagnosis	X	–	–	X
Archiving	X	X	–	X
Comments on the diagnosis	–	X	–	X
Images in the documentation	X	–	–	X
Interim reports	–	–	–	X
Video in the documentation	–	–	–	X
Patient Registration	–	X	–	X
ERP (Electronic Health Records)	X	X	X	X
Account Creation	–	X	X	X
Recipes	–	–	–	X
Data Conversion	–	X	–	X
Emergency information	–	–	–	X
Medical practices	–	X	X	X

In (Fig.2) the differences between compatibility and interoperability are presented. The different types of interoperability implementation are classified in terms of the degree of automation of the process of controlling and extracting the semantic context from the data exchanged:

- **Functional** (technical) interoperability. In this type of interoperability, data exchange takes place at the lowest level in the communication model, providing only a standard for basic data exchange services. Standardize procedures, business processes, document flow, user cases.

It is characteristic of this type of interoperability that semantic compliance cannot be controlled and implemented with digital information technologies.

- **Syntactic** (structural) interoperability. This type of interoperability concerns the mechanisms for packaging and transmission of information. In this case, technical compliance regarding the structure of the messages and the values contained therein is preserved, but there is no possibility to guarantee or control their semantic compliance.

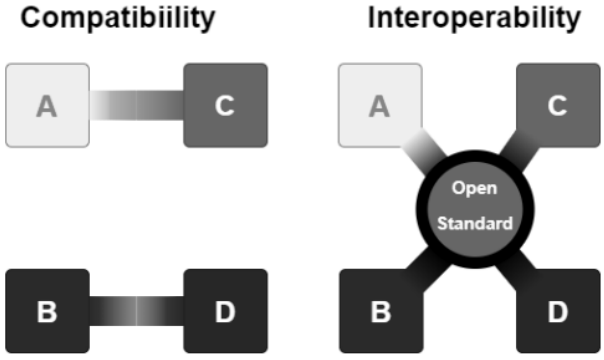

Fig. 2 Compatibiility Interoperability

This form of interoperability shall be effective where the clinical or operational objectives and meaning of the data do not change in the sending and receiving Parties. Because the content of a structured message may not be standardized, this layer does not allow higher levels of understanding between systems. Means (parsers) are used to convert linguistic content, where the chosen communication language sets the standard for natural language data exchange (doctors are able to retrieve electronic documents presented in their original language). It is characteristic of this type of interoperability that, like functional interoperability, semantic compliance cannot be controlled and implemented with digital information technologies.

- **Semantic** interoperability. This is the highest level of interoperability. It characterises the ability of information systems to exchange and understand the semantic context in the data exchanged. In this case, the data have not only a standard structure, but also contain coded elements to represent the semantic context in an indisputable way. Systematized nomenclatures of terms and classification systems (ontologies) of diagnoses, activities, clinical conditions such as SNOMED-CT [4], ICD-10 [5] and LOINC [6] are used for coding. Coding semantic context allows knowledge sharing at the level of clinical concepts. In this type of interoperability, semantic compliance is correctly perceived, both by end-users and through digital information technologies.

2.3. Information models using a database

Information models using messages in clinical data exchange are being developed by Health Level 7 (HL7) [7]. HL7 is an international standards development organization created to meet the increasingly apparent need for interoperability between rapidly advancing medical information systems in the United States since the 1980s. The name of this organization (Health Level 7) is associated with the application seventh layer of the Open System Interconnection (OSI) model for communication between individual computer systems. The OSI model consists of seven layers, where the top three layers are relevant to working with applications, and the bottom four layers carry data over the computer network. Initially, the organization focused on interoperability between large hospitals, and subsequently the target group expanded to those related to the healthcare system. This led to the creation of the first standard for a protocol for the exchange of EPOs (Electronic Health Record) over a computer network. Following this protocol, it becomes possible for such clinical data exchange to take place between any two healthcare information systems that implement this communication protocol. Besides standards for the exchange of clinical data (HL7 v2, HL7 v3, FHIR) are oriented towards the use of messages, HL7 creates standards for the presentation of clinical documents such as the HL7 Clinical Document Architecture (CDA) standard [8]. CDA is a standard for representing the structure and semantics of clinical documents in XML format and belongs to the group of HL7 v3 standards.

Despite their wide popularity, international HL7 standards have inherent limitations in the exchange of clinical data between heterogeneous information systems in medical informatics. These limitations are related to the representation of semantic context, such as the combined use of structural components and coded terms, in which logically unsound interpretations of clinical information occur. Data exchange with HL7 often requires configuration specific to each two systems involved in the communication process. In the course of its development, the standards from the HL7 stack are changing mainly in terms of clinical data management.

2.3.1 Information model of HL7 v2

These are one of the first HL7 information models for data exchange between different health information systems. They are known as the HL7 v2.x group of standards. These standards originated between 1988 (HL7 v2.0) and 2011 (HL7

v2.11) as a means of a virtually convenient approach to exchanging, integrating and managing clinical data generated in clinical observations, laboratory tests, pharmacies, medical devices and insurance events. The purpose of HL7 v2 is to facilitate communication in the field of health services. In particular, the aim is to create clear standards for the exchange of data between medical information systems by removing or significantly reducing program-specific interfaces and their subsequent maintenance. The most common versions are the 2.3 and 2.3.1 versions of the HL7 v2. In 2019. work started on upgrading the HL7 v2 standard to HL7 v2+ [9]. HL7 v2 is one of the most common interoperability standards in healthcare worldwide. In the process of creating the different versions of the HL7 v2 standard, it has been continuously improved without changing its basic principles. This is a standard designed primarily for reliable sharing over a computer network of large volumes of data structured according to a predefined format.

Data transfer over the computer network uses the TCP/IP protocols according to the OSI model. In this approach, data is packaged in message form in the seventh layer of the OSI model, and so these messages are exchanged between computer systems over the network that connects them. HL7 v2 defines a set of rules for sending characters to text in groups representing patient identifiers, clinical identifiers, laboratory test results, other clinical and administrative data. This standard pays attention to the rules for transmitting and receiving data values and observing the sequence of transmitted messages by processing 37 data transfer errors that may occur in the Application Seventh Layer of the OSI model. The rules for the exchange of data shall cover the following actions:

• Message formatting. These are rules that determine how to compose a message and how to structure the elements in a message.

• The transmission of messages. These are rules that determine how systems send and receive messages, how their acceptance is confirmed and the extraction of message data.In HL7 v2 are standardized messages used to perform typical activities in almost every area of healthcare. The standard specifies the concepts for building messages, the structure of individual message types and syntax for recognizing individual parts in messages. On (Fig.3) the basic concepts in HL7 v2 for message representation are schematically presented.

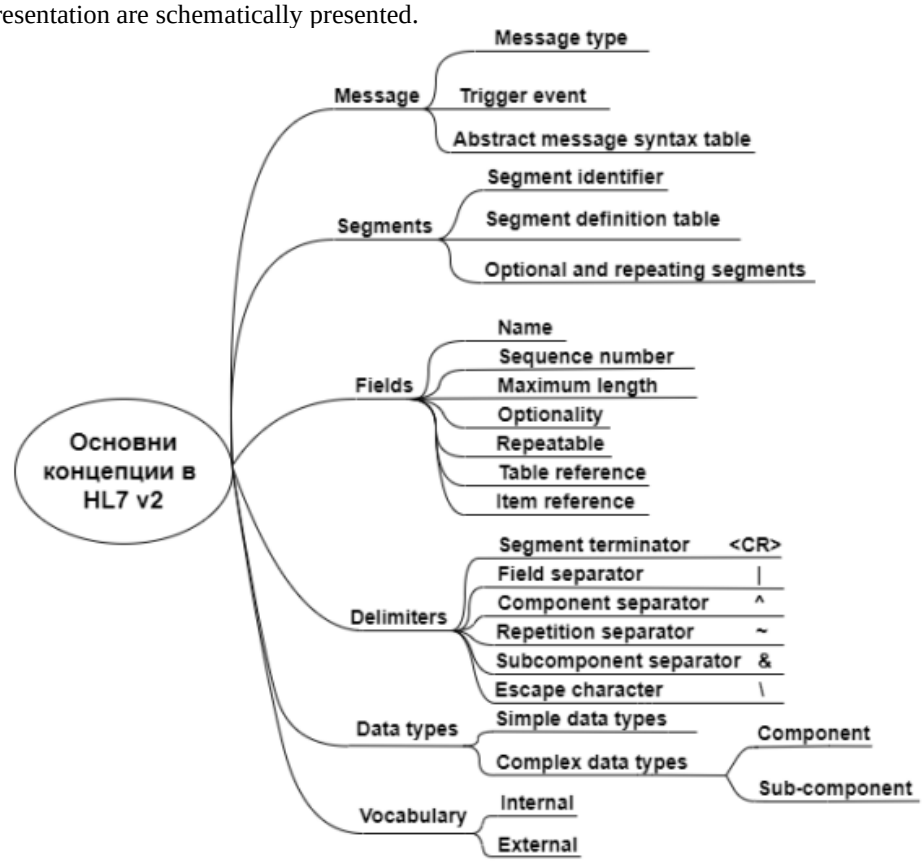

Fig. 3 Schematic of the basic concepts in HL7 v2 for message representation

Each message has a certain type and is composed of one or more segments in a specific sequence. Messages in HLv2 are sent in response to events (patient admission, laboratory tests received, patient discharge, etc.). Message types in HLv2 are defined in relation to the events that give rise to them. The list of types includes Admission, Discharge and Transfer message types, known as an ADT message, Order Entry delivery, Medical Review Report, Test Results, Vital Signs (Observation). Reporting).

For example, the ADT message would contain data about the address registration of the patient, the reason for accepting treatment, the data of the doctor who performed the intake of the patient, etc. In turn, each segment consists of fields, the sequence of which is also strictly defined. Fields can contain different types of data. Всеки сегмент съществува независимо от останалите. Each segment exists independently of the others. Some of the segments are mandatory for a certain type of message, while others are optional. Segments are identified by a code consisting of three

characters (segment identifier). Identifiers of segments starting with the letter Z are considered user-defined segments (so-called. Z message segment). Segments are reusable components of a message containing information according to the message type. For example, the address registration segment can be used in many other scenarios. For this reason, HL7 v2 defines a large number (over 100) of segment templates that cover user cases from financial transactions to changes in hospital bed status. Each segment consists of one or more data fields. Each field is characterized by a certain type of data. Data types can be simple, single-valued, or multiple, with one or more component fields.

Composite (composite) data types can contain both simple and other composite data types as nested components. (Fig.3). Since the message should be as short as possible, the field names are encoded with specially specified by the standard (over 1700 codes) and exceptionally it is possible to additionally use user-defined codes. For example, a field name Message header is represented by MSH, Male is represented by M, etc. Differentiation of the fields in the segment is achieved with control symbols (separators, Delimiters) shown in (Fig.3).

2.3.2 Information model of HL7 v3

HL7 v3 [10] is one of the newer interchange-oriented standards of HL7, which aims to avoid the shortcomings identified in HL7 v2. For this purpose, an objectoriented methodology (UML) and a reference information model (RIM) are used to create the messages. The RIM of HL7 v3 is essentially used to represent the semantic and verbal relationships existing in the information carried in HL7 messages. A Data Type Specification and a Set Specification of all concepts used for data type coding or properties are also introduced. This aims to reduce the optional components in messages, increase the rate of multiple use of components and improve the logical connectivity of data in messages. First of all RIM defines the message syntax of this standard, the permissible relationships between elements of the message representation language and data types. However, RIM cannot be defined as a model from medical informatics, although it is oriented towards this applied field. At the heart of RIM are three main classes (Act, Role and Entity) related to the classes ActRelationship, Participation, Entity-Role and RoleLink (Fig.4), among which the most commonly used are the instances of the Act class (analogous to a verb in natural language). Each Act object can have any number of Participation objects, which are Role (roles) executed by Entity (categories). Participation objects are analogous to nouns in natural language. Act, Role, and Entity classes can have 44 derived classes.

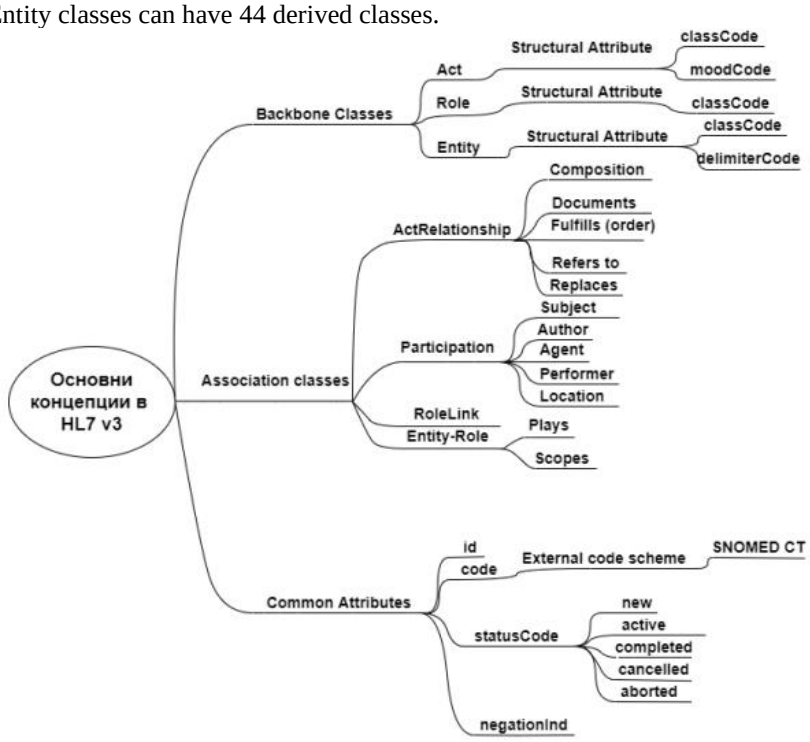

Fig. 4 Schematic of RIM in HL7 v3

The great advantage of this standard over HL7 v2 is the introduction of RIM, the object-oriented technologies for building the message models and the presentation of messages in XML format. On the other hand, achieving semantic interoperability with this standard is still an unresolved problem, as there remain open possibilities for violating the model constraints, no tracking of different versions of the model is provided and it is difficult to create a chain of validity checks against a set valid model.

2.3.3 Information model of HL7 FHIR

HL7 FHIR (Fast Healthcare Interoperability Resources) was launched in 2011 and combines successful solutions from previous versions with a completely new philosophy, architectural concept and open approach to the design and development of the standard. At the heart of the standard are FHIR resources. The resource is an independent, structured unit of information used in the exchange of medical data. Most resources are real-world representation in digital data. Examples of resources are: Patient, Review, Diagnostic Report.The specification describes clinical, administrative, financial and technical resources. Currently, the standard lists 106 resources.

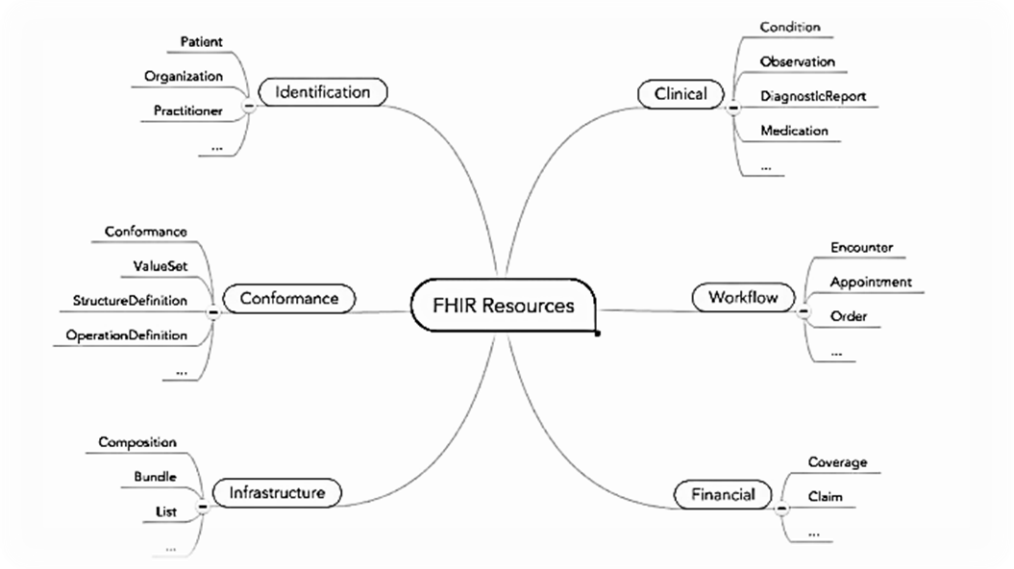

Fig. 5 Outline of the basic concepts in HL7 FHIR

Each resource is described by a set of standardized attributes (elements), in addition to which each resource has a built-in expansion mechanism (Fig. 5). Each resource has a section for presenting structured information contained in the resource in human-readable form. This section is used to ensure interoperability at the most basic level, that is, having received such a resource, you can always display its contents to a person on the monitor screen, for example, in a browser, without further processing and storage of data in your storage in a discrete form.

The HL7 FHIR specification describes several supported approaches to intersystem communication. Systems can share resources individually or merge related resources into packages and share those packages. The possibilities for organizing the data exchange are:

- **RESTful API** (HTTP) – the interaction between systems takes place by performing operations on resources using REST requests (finding a resource, receiving a resource, updating a resource, etc.)
- **Messages** – Communication between systems is organized in the form of sending messages between systems. Each message contains information about an event that has happened, reflected in the information system and about which one system wants to inform the other. A message is a group of related resources of a specific type (message).
- **Documents** – Communication between systems takes place at document level, i.e. one system requires documents from another system and receives them. A document is a group of resources that are grouped into a document using a special composition resource and pinned at the time the document is signed. Depending on the architecture of your solution, the challenges you solve, and the detail you need when sharing health data, you may be able to use the appropriate sharing option.

Resources within the HL7 FHIR are logically closed blocks of data that are intended for exchange. By default, each resource has a small number of restrictions on mandatory items and ValueSets. In real-life situations, you may want to pin some data as mandatory. For this purpose, the mechanism for profiling resources is used. By using a special Structure Definition resource, you can create a profile for each resource in the specification, thereby setting limits for it:

- **Structure –** Mandatory data elements
- **Dictionaries** – The set of values used for a specific resource element. Profiles (Structure Definition), like all other resources, are accessible through the RESTful API, so each system can retrieve both the data resource (e.g., Patient) and the profile it corresponds to. In this regard, systems that support HL7 FHIRs can be "taught" by other systems with which data is exchanged. Similarly, operations performed on resources (RESTful APIs) can be profiled. To do this, use the Operation Definition resource in which the new operation can be described. Using this activity profiling mechanism, we can define new operations and thus extend the standard set of operations specified in the standard.

As a summary, it can be said that with regard to the future of standards: V2 is no longer being developed, V3 takes a long time to develop, and FHIR is being developed quickly and trying to preserve the main successful concepts of HL7 V3, simplifying them as much as possible and being actively promoted by HL7 itself. so it is a natural choice to implement. The FHIR standard is able to solve all the problems for which the earlier standards than HL7 (HL7 v2, HL7 v3 and CDA) were used. In most cases, FHIR has additional advantages, especially when it comes to ensuring compatibility. The FHIR standard is therefore likely to gradually replace some or all of these standards. However, it is not yet clear how quickly the mass transition to FHIR will take place. It is likely that current standards will be applied in parallel with each other. HL7 International decided to maintain existing standards for as long as the community needed. [11]

III. OBJECT, SUBJECT, AND METHODS OF RESEARCH

The object of this study is the development of a affordable from a price point of view device used to measure the lung function of a person at home. The developed prototype spirometer (Fig.6) is an instrument for measuring peak exhaled air velocities at initial maximum inhalation. It is possible to make accurate measurements of certain respiratory functions

by means of the instrument. The spirometer is equipped with a differential pressure sensor which contributes to reducing fluctuations and eliminating the gravitational impact of flow measurements made by the device. As a result of the increased sensitivity of the spirometer and its respiratory measuring apparatus, more complex and useful statistical measurements can be made, such as one and six seconds of forced expiratory volume measurements (FEV1 and FEV6, respectively).

Through its integration into an information-measuring complex based on a personal computer workstation, with the proposed implementation of the spirometer, biomedical (respiratory) data can be registered and transmitted to the workstation, to create an electronic diary, analyzed using expert systems based on artificial intelligence (AI) or transmitted to a doctor for detailed interpretation.

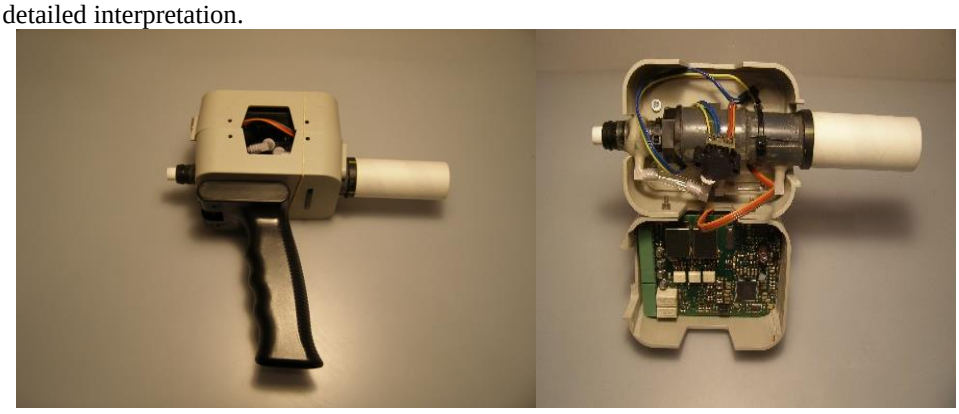

Fig. 6 Technical implementation of a portable spirometer

The presented prototype of a spirometer consists of several main elements:

• *breathing tube* through which the patient breathes freely. As a result of a small, previously known aerodynamic resistance of the pipe between its beginning and end, a certain pressure difference is created, which is directly proportional to the volumetric flow rate of the air. This difference is captured by:

• *differential pressure sensor*, so it is possible to register changes in the volumetric flow rate of air during inhalation and exhalation - pneumotachogram. The differential pressure sensor directly converts the pressure difference from the beginning and end of the tube into an electrical signal (voltage) The information is then sent to the:

• *microcontroller* for electronic processing containing the amplifier (A) and ADC. In this case, the signal must first be passed through a digital filter (DF). If necessary, the filtered signal passes again through the amplifier and enters the processing unit (processor), where static, dynamic lung volumes and forced ventilation flows (VC, FEV1) are calculated (Fig. 7). The data obtained can be displayed on the doctor's monitor in the form of a "flow-volume" loop.

The registered biomedical information at the next stage can be transmitted through a communication channel (Internet) to an expert system implemented on the basis of the Azure IoT Suite cloud platform.

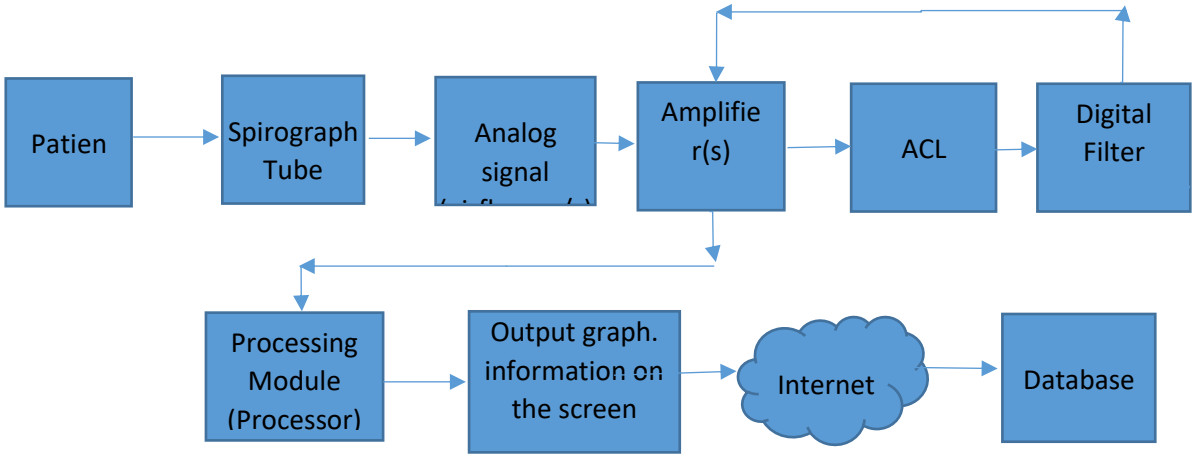

Fig. 7 Block diagram of the operation of a spirometer

After the primary processing of biomedical signals, the analysis of data in monitoring systems is most often carried out on the basis of microprocessor platforms based on technologies that open great opportunities for the implementation of complex diagnostic algorithms for processing physiological information. In such microprocessor platforms, algorithms for spectral, statistical, regression and other programmatic techniques implementations of mathematical analysis are applied.

Digital signal processing in microprocessor systems provides a broad opportunity for modern screening systems to conduct complex, very parameter analysis of incoming biomedical information.

Telemedicine combines excellence in high technology with state-of-the-art advances in medical diagnostics. Telemedicine is a complex of medical services and activities that use technologies to deliver medical care at the site of need. The components of telemedicine are:

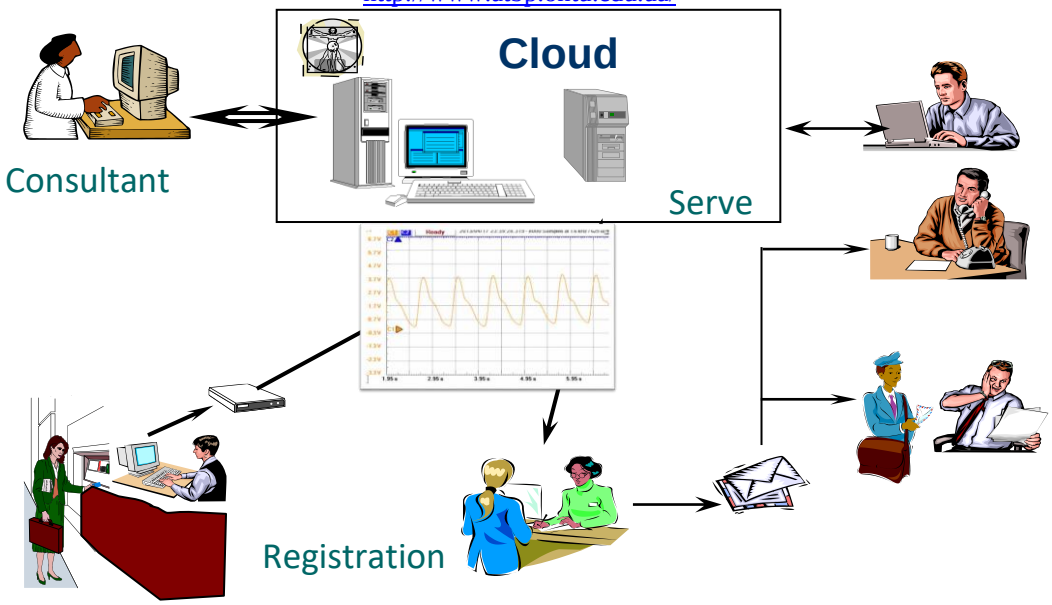

Fig. 8 Schematic of connections in a telemedicine system

- Technical devices for recording, storing, processing and transmitting medical information.
- Technologies for medical decision-making.
- Experts for interpretation and evaluation of specialized medical information.
- Bilateral conferencing and real-time agreements.
- Managing and discussing the patient.

IV. CONCLUSIONS

Undoubtedly, further research in the development of clinical screening and monitoring systems will lead to new results important for solving the problems of building a more sophisticated monitoring technique and solving real problems in diagnosing the human condition. The task of obtaining reliable biomedical information is a major element in the development of biomedical electronics, especially from the point of view of the possibility of implementing telemedicine services.

In the use of modern information and communication technologies, the reliability and security of medical, biomedical and biometric information is a very important element in deciding on their use. From the point of view of cybersecurity, when implementing such systems and services, the technological solutions that cloud-based structures offer for managing smart appliances and embedded electronic systems are of paramount importance. Azure IoT Connector for FHIR, using the HL7 specification, enables reliable and secure biomedical data exchange in the implementation of IoT-based telemedicine systems.

V. REFERENCES

[1] https://ipmagazin.bg/bg/news/164/kakvo-e-biometriia-i-biometritchni-danni.
[2] Д. Чаръкчиев, "Информатизирано Здравно Досие. Електронен Здравен Запис. Лекция по Информационни системи в здравеопазването," Факултет по Математика и Информатика. СУ Св. Климент Охридски, София, 2018.
[3] https://effect.habr.com/a/LVPLv2UY3_au-azgqV-uV7ghb5oY2KPlCA6QSarvMixLeODfsIZYig6JdpbBZljlB2KWCseqJHwck1AKw3IqpH1pUhJ9wi_fNp57gqfhoacaXwiEd2S1Izzne7LY
[4] SNOMED-CT, "SNOMED International," 2019. [Online]. Available: https://www.snomed.org/.
[5] ICD-10, "International Statistical Classification of Diseases and Related Health Problems 10th Revision," World Health Organization, 2016. [Online]. Available: https://icd.who.int/browse10/2016/en.
[6] LOINC, "Logical Observation Identifiers Names and Codes," Regenstrief Institute, Inc., 2019. [Online]. Available: https://loinc.org/. [Accessed 3 June 2020].
[7] T. Benson, Principles of Health Interoperability HL7 and SNOMED, Springer-Verlag London Limited, 2010.
[8] HL7, "HL7 Products - Master Grid," 2020. [Online]. Available: http://www.hl7.org/implement/standards/product_matrix.cfm. [Accessed 22 June 2020].
[9] HL7, "HL7 v2+," HL7 International, 28 April 2020. [Online]. Available: http://www.hl7.eu/refactored/hl7.html. [Accessed 15 June 2020].
[10] HL7, "HL7 Version 3 Product Suite," HL7 International, 30 Jan 2017. [Online]. Available: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=186. [Accessed 22 June 2020].
[12] https://studfile.net/preview/14964596/page:3/

Отримана в редакції 26.07.2024. Прийнята до друку 17.08.2024. Received 26 July 2023. Approved 17 August 2024. Available in Internet 23 October 2024