Abstract—The objectives of the present study are investigation, assessment and evaluation of data security and patients’ privacy in a real-time wireless telemedicine system utilising GSM/GPRS, BLUETOOTH protocol, and a cellular phone. Fifteen non-risky heart patients, aged (49±14) years (9 females, 6 male) were recruited. The ECGs were continuously monitored (72 h) and transferred anonymously; assigning each patient an identification number and monitoring start time and date, while the patients were performing their every day’s indoors and outdoors activities. The data were collected and processed by a modem server at hospital. The server was assigned user-name and password, which were known only by the in charge health care personal, and the ECGs were identified only by patients’ id-number. Authentication, confidentiality and integrity of the data were tested for the risk of Insertion attacks, Client-to-client attacks and Misconfiguration. No access by unauthorised person was possible to neither mobile phone, nor the Bluetooth module which controls connection establishment and termination, data flow and dial-up communication. No access was possible for unauthorised person at server side and nor the ECG could be personalised. In the present setup, which clinical application is implemented in a small scale, the ECG data is secured and patients’ privacy is achieved.

Index Terms— Data security, healthcare, patient’s privacy, wireless remote system.

I. INTRODUCTION

The prospect of transferring and storing health information in electronic form raises concerns about patient privacy and data security. Data security and patients’ privacy in medical remote monitoring system are two important aspects, which should be explored and regulated. Security relates to the means by which an entity protects the privacy of any information, and it depends very much on the applied communication technology and data processing. Privacy refers to the individual’s right to keep certain data or information private, unless that information will be used or disclosed with his/her permission.

The rapidly emerging infrastructure of health care information and its relation to patient privacy have been described in the literature [1][2][3]. Authentication, confidentiality and integrity of the transferred information are minimum requirements any patient will demand [4].

Privacy includes topics such as: the scope of healthcare providers who must comply, consent and authorisation issues/procedures, right of individuals, organised healthcare arrangements and business associated requirements. Security and privacy are very much intertwined; indeed this is security that assures the privacy.

Telemedicine is used for disease management, patient consultation, patient monitoring and patient care. In a modern healthcare service, where the health authorities tend to optimise the resources most effectively, it is in many cases an advantage to treat/monitor as many patients as possible at their home. While the patients are understandably concerned about the privacy and security, prefer being treated/monitored in their home (more natural environment), as it is more convenient for them. However, systematic transmission and collection of a broad range of medical data can present a substantial tradeoff in loss of personal privacy [5].

Wireless communication, contrary to wired communication, is more likely exposed to eavesdropping. Therefore, the transmitted medical data should be impersonalised and no one should have access to that.

The present paper explores data security and patients’ privacy in a wireless remote patient monitoring system [6][7][8] in a clinical setup.

II. MATERIAL AND METHOD

A wireless remote patient monitoring system (Figure1) consisting of a patient-unit (an ECG device, a Bluetooth module and a Mobile phone), public GSM/GPRS network, a GSM/GPRS modem server, and a graphical monitoring station were arranged and setup. To make the mentioned setup functioning in a reliable manner with god performance a generic communication platform based on Bluetooth and GSM/GPRS protocols were designed, developed and integrated [6][7][8]. Fifteen non risky heart patients (n = 15), aged (49±14) years (6 males and 9 females) were recruited.

The patients’ ECGs were continuously monitored (72 h), while they were performing their every day’s indoors and outdoors activities. Following the instructions, the patients wore the patient-unit, mount the disposable electrodes.
operate, and changed or recharged the batteries, if needed, by
own self.

For safety reasons, the patients had a fixed telephone line at
home and were equipped with an extra mobile phone when
they were out of doors, and they were promptly contacted in
case there was any technical or health problem [8]. Taking
shower or swimming, while wearing the patient unit, was not
permitted.

The ECG data was transferred anonymously via
Bluetooth-GSM/GPRS connection in packet format, assigning
each patient an id-number, start monitoring time and date. No
name, personal id-number, age, or address, were transferred
along with the ECGs. Only healthcare personal knew whom
each ECG was belonging to. The data were collected and
processed by a modem server at destination side. The
illustrated ECGs in the graphical interface, on the server side,
were identified by patients’ id-numbers. The server was
assigned a user-name and a password, which were known
only by the in charge health care personal.

Data security from the technological point of view was
investigated [6]. The applied telecommunication technologies
and services (Bluetooth, GSM and GPRS) offered Access
Control, Authentication, Data Encryption, and User
Anonymity. The privacy and security of the transferred ECGs
were judged by a committee consisting of three competent
persons who were blind to the experiments. The present
wireless remote patient monitoring system was inspected and
examined in order to explore any possible intrusion from
unauthorised persons and to unveil any possible
impersonalised ECG data. In this relation the authentication,
confidentiality and integrity of the data were tested for the risk
of Insertion attacks, Client-to-client attacks and
Misconfiguration.

III. FUNCTIONALITY

The ECG signal is collected, via 4 disposable electrodes,
by an ECG device. The ECG device is connected to a
Bluetooth module, which transferring data via Bluetooth
connection to a mobile phone (figure 1). The Bluetooth
module invokes the mobile phone as soon as the ECG device
has detected the electric activity of the heart. The mobile
phone establishes a GSM or a GPRS connection to the public
mobile network automatically.

The transmission of data, from mobile phone to Modem
Server at the hospital, is carried out in real time and
continuously in packet format. The Modem Server receives
the data and converts it to a pre-defined format. The data then
are sent to the central monitoring station via a serial cable.
Central monitoring station interoperates and converts the
received data to graphical ECG [6][7][8].

The mobile phone is connected in the course of the real-
time monitoring period. In case the network fall down or no
GSM/GPRS network coverage, the Bluetooth module
automatically, via the mobile phone, repeatedly attempts for
connection reestablishment until a complete connection is
established. The GSM mobile phone is functioning as a
mobile modem to the ECG device after the connection is
established.

Health care personal at the hospital have the possibility
to communicate with the patient by sending him/her text
message (in packet format). In case an audio conversation is
needed, either a mobile phone (an extra one) which is on the
patient outdoors or a fixed telephone at home is used.

IV. THE BENEFIT OF THE SYSTEM

Most of the existing telemetry devices are off-line (Store-
and-Forward Telemedicine) and rely on wired
telecommunication network such as Digital Subscriber Line,
Public Switched Telephone Network and Integrated Services
Digital Network. Even though, very few devices/systems
applying wireless and cellular technologies, those are most
off-line, and the majority use Wireless Local Access Network
and Internet connection, which make these telemetry devices
dependent on a fixed access point and fixed infrastructure.
Although, these telemedicine models have a reasonable
performance but need a great deal of preparation from the
network provider side before any application, as regards
installation and logistics. Moreover, these models limit users’
movement freedom and bound them only to their home
environment and very close surroundings. This telemedicine
setup needs also sophisticated security management, as
hackers can easily intrude the internet and access vital
patient’s information.

One of the main factors that make a telemedicine system
a success is the use of a secure modern communication
technology.

The designed and implemented telemedicine model in the present study employs advanced wireless and mobile technologies (Bluetooth protocol, and TCP/IP connection over GSM and GPRS) utilising the existing public cellular network [6]. One the main benefits of this model is that there is no need for any preparation regarding installation and logistics from the network provider side, and the patients need only a short instruction in the employment of the telemedicine device at the hospital/health centre before using it [8] and application of a mobile phone is more common in these days. The second benefit is that the patients are not bounded to their home environment and surroundings, and they can move wherever there is network coverage, thus the telemedicine device is not dependent on a fixed infrastructure. Moreover, the system takes advantage of using the solid security arrangement build in the Bluetooth, GSM and GPRS security protocols. Hence, the present model guarantees as well the Portability as the Accountability of the system.

V. RESULTS

Without knowing user-id and password of the patients on the patient side, no access was possible; the Bluetooth module which controls connection establishment and termination, data flow and dial-up connection could not be accessed by any unauthorised person as well. No received ECG could be personalised at the server side.

The achieved results could not be generalised, since the present remote patient monitoring system was tested on limited number of patients (n = 15), only few health care providers were involved (n = 4), and the system was tested only in one specific healthcare environment with specific security and privacy policies. However, the applied approach for security and privacy measurement was basic and fundamental; hence the used method is valid.

VI. DISCUSSION AND CONCLUSION

While Information Technology (IT) enables the use of security arrangement in medical remote monitoring system to limit access to confidential information, it also introduces some real vulnerability. Unless proper controls and procedures are implemented, these kinds of applications also invite unauthorized users to access the data. If the concerns are not sufficiently addressed, the health care consumers will hesitate to share information. Therefore, IT application development and use of that in remote monitoring system must be done in the midst of maintaining confidentiality, privacy, and security.

The presented system is reliable, functions with a clinically acceptable performance, and transfers medical data with high quality, even though the system was tested under totally uncontrolled circumstances during the patients’ daily activities [8]. In the present setup, which its clinical application is implemented in a small scale, the ECG data is secured and patients’ privacy is achieved.

However, in a large scale, where larger number of patients is involved, several health care providers are in charge, data magnitude is huge, and the setup is tested in several health care centres with deferent infrastructure and different security policy, then data security standards for management of authority access, coding, and structure must be developed. These are the challenges in a future research.

REFERENCES