# Personal and Sensitive Data in the e-Health-IoT Universe

Fiorella Guadagni[1], Noemi Scarpato[1](✉), Ferroni Patrizia[1],
Grazia D'Ottavi[2], Fernando Boavida[3], Mario Roselli[4],
Graziano Garrisi[5], and Andrea Lisi[5]

[1] San Raffaele Rome University, Via di Val Cannuta, 247, Rome, Italy
{fiorella.guadagni,noemi.scarpato,patrizia.ferroni}
@unisanraffaele.gov.it
[2] San Raffaele S.p.A., Via Androne 81, Catania, Italy
grazia.dottavi@sanraffaele.it
[3] University of Coimbra, Coimbra, Portugal
boavida@dei.uc.pt
[4] University of Rome "Tor Vergata", Viale Oxford 81, Rome, Italy
mario.roselli@uniroma2.it
[5] ANORC - National Association for Digital Preservation Officers and
Operators, Via Stampacchia 21, Lecce, Italy
{grazianogarrisi,andrealisi}@studiolegalelisi.it

**Abstract.** Internet of Things (IoT), smart objects, are today part of our life and used in almost every industry and human activity: from e-health to e-learning not forgetting home automation and wearable technology. IoT promises to change our lives to make them easier, more efficient and "smart", however, we are now facing major challenges: security, data protection and privacy.

**Keywords:** IoT · Privacy · Informed consent · Security · Jurisdiction

## 1 Introduction

The market of IoT is exploding and many studies have deeply analyzed and defined the IoT architecture [1–3]. IoT promises to change our lives to make them easier, more efficient and "smart", however, we are now facing major challenges: security, data protection and privacy.

Article 29 of Directive 95/46/EC set up a Working Party (WP), an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. In September 2014, the WP has issued the present opinion: "Opinion 8/2014 on the Recent Developments on the IoT" (WP223, adopted on 16 September, 2014) which focuses on three IoT developments: wearable technology, quantified self and home automation. This because, as stated by the WP in the Scope of the opinion, at the present time it is impossible to predict "*with certainty*" the extent of future IoT development due to fact that it is still an open question how all the data collected with IoT could be transformed.

B. Mandler et al. (Eds.): IoT 360° 2015, Part II, LNICST 170, pp. 504–514, 2016.
DOI: 10.1007/978-3-319-47075-7_54

WP223 [4] should be read in connection with previous opinions adopted by the Working Party "on the application of the concepts of necessity and proportionality and data protection in law enforcement" (WP211) and "on surveillance" (WP 215), as well as "on apps on smart devices" (WP202, 2013), Opinion 4/2007 "on the concept of personal data" (WP 136, 2007) [5] Opinion 01/2010 "on the concepts of controller and processor" adopted on 16 February 2010 (WP 169) [6], Opinion 05/2014 "on Anonymisation Techniques" adopted on 10 April 2014 (WP 216) [7], Opinion 5/2009 "on online social networking" adopted on 12 June 2009 (WP 163) [8], Opinion 13/2011 "on Geolocation services on smart mobile devices" adopted on 16 May 2011 (WP185) [9], Opinion 15/2011 "on the definition of consent" adopted on 3 July 2011 (WP187) [10].

The first sentence of the WP223Summary states: "*The Internet of Things (IoT) is on the threshold of integration into the lives of European citizens. The viability of many projects in the IoT still remains to be confirmed but "smart things" are being made available which monitor and communicate with our homes, cars, work environment and physical activities.*"

A succeeding statement stresses a crucial point: "*Many questions arise around the vulnerability of these devices, often deployed outside a traditional IT structure and lacking sufficient security built into them. Data losses, infection by malware, but also unauthorized access to personal data, intrusive use of wearable devices, or unlawful surveillance are as many risks that stakeholders in the IoT must address to attract prospective end-users of their products or services.*"

The WP highlights that "*users must remain in complete control of their personal data throughout the product lifecycle, and when organizations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific*" and continues stating that "*Indeed, empowering individuals by keeping them informed, free and safe is the key to support trust and innovation, hence to success on these markets.*"

The WP has identified six "*significant privacy and data protection challenges related to the Internet of Things: Lack of control and information asymmetry; Low-quality consent; Extrapolation of inferences from data and repurposing of original processing; Intrusive identification of behavior patterns and user profiling; Limitations on the possibility of remaining anonymous whilst using services; Security risks*".

Data exchanged through the IoT infrastructures could be private. For this reason, it is mandatory the platform must ensure privacy and security. It is important to note that privacy is not only a technical property but is an aggregation of a legal, socio-ethical and technical viewpoints. The legal regulation on privacy, especially when dealing with relevant health data (as in e-health), presupposes the application and respect not only of the legislation that is the main reference "Directive 95/46/EC" of the European Parliament and of the Council of 24 October 1995 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (also called "Data Protection Directive (95/46/EEC)", but also a series of specific measures and guidelines (all linked together, due to the often absence of specific legislation) issued by the Authority for the protection of personal data.

Moreover, we should also consider the "European Parliament legislative resolution of 12 March 2014, on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM (2012)0011–C7-0025/2012–2012/0011(COD)-(Ordinary legislative procedure: first reading). This new European legislative resolution contains some important principles and rules of proper treatment and will replace all the individual national legislations of the EU member countries. A consolidated version of the first reading of this new European regulation can be found linking to [11]. At the time of this paper edition, the European Parliament is proposing 207 amendments, some of them crucial for IoT projects (e.g., amendment #95).

Although some security [12] and privacy [13] approaches have been proposed, IoT still raises several security and privacy challenges that must be addressed. In this paper we will analyze some critical issues related to privacy aspects in IoT architecture and consequent main legal requirements considering as a paradigmatic example the Italian Privacy Code.

## 2 Legal Scenario

Due to the sensitivity of data that may be processed, the regulatory perimeter within which it is possible to proceed with the development of IoT systems and the classification of information and documents that can be treated in different contexts (e-health, cloud, etc.) should be defined, through a phase of analysis of the main legal requirements concerning privacy. Preliminarily, therefore, it is necessary to evaluate:

- the requirements and the stakes imposed by the regulations;
- the compliance with the general principles and organizational measures and safety (according to the principles of privacy by design and privacy by default, further specified);
- the conformity of the treatment performed with new tools compared to current regulation;
- the severity of any discrepancies and the consequent urgent resolution,
- the possible sanctions in case of non-compliance with the requirements of legislation and with the measures of the Data Protection Authority (DPA).

The legal regulation on privacy, especially when dealing with relevant health data (as in e-health), presupposes the application and respect not only of the legislation that is the main Italian reference, Legislative Decree no. 196, 30 June 2003, “Code regarding the protection of personal data” (so-called Privacy Law) and its Annex B (Technical regulations regarding minimum security), but also a series of specific measures and guidelines (all linked together, due to the often absence of specific legislation) issued by the Authority for the protection of personal data.

In fact, the special attention given by the Lawmaker to the proper handling of personal data, especially sensitive ones, necessarily implies the performance of a whole series of requirements both organizational and technical security measures. From this legislation comes down a series of requirements, all of which occur in the management and treatment of personal data and that can be divided into:

- **General requirements** (disclosure ex Art. 13, right of access ex Art. 7 and eventual acquisition of consent to data processing in accordance with art. 23);
- **Special requirements** (notification to the DPA in cases specifically indicated in art. 37 and questioning or preliminary verification pursuant to Article 17, if the processing of some data might represent a specific risk for the person concerned);
- **Organizational requirements** (minimum security measures, necessary and appropriate, regulated by Articles 31 and the following, and by specific provisions of the DPA, especially with regard to the processing of data in health setting).

Compliance with these requirements is considered necessary in the development of a IoT architecture and in subsequent use in reference to identified or identifiable individuals. Nevertheless, privacy protection should not disregard defense instruments that not only prevent accidental loss of data, or the external non-authorized access, but also preserve the digital memory in time of the scanned documents.

In general, there are four main requirements that must be put in place in order to properly proceed with the processing of personal data: (i) notification to the DPA (if necessary); (ii) communication of the information to the individual; (iii) acquisition of the consent to treatment; (iv) establishment of minimum, necessary and appropriate security measures for the processing of personal data.

These concern, in particular, technological and organizational measures aimed at avoiding a treatment of data by unauthorized persons and the loss, destruction or dispersion of data stored in their databases. For this reasons, privacy protections in IoT devices "*should be built-in from the very outset, in application of the "Privacy by Design" principle*" (WP223) and before they are released in the market, a Privacy Impact Assessment should be performed, as detailed in Sect. 2.3.

## 2.1 Principle of Necessity

The main principle of the entire Italian Privacy Code (Legislative Decree no. 196/2003), which should inspire all treatments within the IoT (and, therefore, also regarding the processing of data concerning health) and must be kept in mind in the implementation of technology solutions in these areas, it is the "principle of necessity" (art. 3), which is considered an extension of the old principles of relevance and of no data surplus, compared to the treatment aim and certainly plays the role of general interpretative key for all items of the Italian Privacy Code. Under this principle, anyone dealing with personal data will have to do so to ensure that the personal data themselves can only be used and to the extent that is strictly necessary for the achievement of specific objectives, which in turn will have to be identified and disclosed to the person (disclosure ex Art. 13 Legislative Decree no. 196/2003). As repeatedly stated by the DPA, in the treatment of medical data, for example, all medical devices should be developed and programmed in such a way that this principle is respected from the beginning, also in accordance with the Community framework which sees the application the so called principle of "privacy by design" (i.e., the provision of measures to protect the data already at the design stage of a product or software).

Closely linked to the principle of necessity is the art. 11 of the Code, which develops the basic guidelines to follow during any processing of personal data. According to this article, the basic personal data undergoing processing shall be:

(a) processed lawfully and fairly;
(b) collected and recorded for specific, explicit and legitimate purposes and used in other processing operations in terms compatible with those purposes;
(c) accurate and, where necessary, updated;
(d) adequate, relevant and not excessive in relation to the purposes for which they were collected or subsequently processed;
(e) kept in a form which permits identification of data for a period of time not exceeding that necessary for the purposes for which they were collected or subsequently processed.

## 2.2 New Principles: Privacy by Design and Privacy by Default

In order to protect individuals, therefore, it is necessary to operate in accordance with the new principles of "Privacy by Design" and "Privacy by default", even considering to make a real "Privacy Impact Assessment" in relation to each instrument used. This means that:

- privacy must be incorporated in the design and architecture of IoT systems ("Privacy by design");
- there must be attention to the centrality of the interests of individuals (treat only the necessary data);
- the amount of data collected and the duration of their conservation should not go beyond the minimum necessary to achieve the aims pursued (principle of relevance and limits);
- these mechanisms must ensure that - by default - no personal data are made accessible to an indefinite number of people;
- personal data must be automatically protected in any IT system (taking account of technological and implementation costs);
- if the treatment has risks (by nature, scope or their purposes) the administrator must perform an impact assessment (Privacy Impact Assessment).

### 2.2.1 Privacy by Design

Because privacy must be incorporated in the design and architecture of IT systems, already in the design phase of an information management system, solutions ensuring that they are treated only the personal information necessary for each specific purpose of the treatment, must be provided. Privacy, therefore, becomes an essential and integrated component of the system (without reducing its functionality). To achieve this, the designers and operators should be asked to consider the priority interests of individuals by providing effective privacy default interventions, appropriate information and enhanced user-friendly options to the user.

### 2.2.2 Privacy by Default

Every IT system should ensure that only the personal information necessary for each specific purpose of the processing are treated, by default, and that the amount of data collected and the duration of their preservation does not go beyond the minimum necessary for the purposes sought. In particular, personal data should not be accessible to an indefinite number of people and those involved must be able to control the distribution of their personal data.

## 2.3 Privacy Impact Assessment (PIA)

This activity postulates a series of operations which identifies treatments presenting specific risks (e.g. profiling, special categories of data, data accessible to a vast number of people, large amounts of data or data combined with other data). In this case, the PIA must consider:

- the confidentiality of the individual data;
- the confidentiality of the person (physical integrity, biometrics, body checks, etc.);
- the confidentiality of personal behavior (video surveillance, sexual preference, political, etc.);
- the confidentiality of personal communications (interception, monitoring, email);
- identify the impacts that the project has on an individual privacy and identify less intrusive alternatives;
- assess the impact from the point of view of all stakeholders;
- understand the level of acceptance of the project and its characteristics;
- clarify the needs of the project that have negative effects on privacy and are not avoidable (acceptance of residual risk);
- document and publish results (PIA reports).

PIA, therefore, involves:

- a systematic description of the proposed treatment, its necessity and proportionality in relation to the objective pursued;
- an assessment of the risks to the rights and freedoms of data subjects;
- measures to address the risks and minimize the volume of personal data;
- safeguards, security measures to ensure the protection of personal data and demonstrate compliance with current legislation, taking into account the rights and legitimate interests of the data subjects.

All this can be also realized by means of a Privacy Impact Assessment, which focusing on risk management and securing compliance with the requirements of the legislation on data protection and privacy, will give us back a specific assessment of the privacy implications of developed programs or new activities to be undertaken.

### 2.4 Data Subject's Consent

The data subject's consent is one of the legal basis for the processing of personal/sensitive data. This aspect is becoming more and more relevant considering that in a few years, IoT devices will be a major generator of "big data" at a very high velocity. We are at a stage where data generated by IoT meet the 5 V's: Volume, Variety, Velocity, Variability and Value [14]. In this perspective, data subject should be aware of it and should be able to completely control the all lifecycle processing of her/his personal data.

The definition of Consent was set by the Council Common Position10 in 1995, as "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*".

When consent is requested to processing personal data health-related in electronic health records (EHR) a specific consent must be obtained, as stated in WP131 - Working Document on the processing of personal data relating to EHR: *"Specific" consent must relate to a well-defined, concrete situation in which the processing of medical data is envisaged. Therefore a "general agreement" of the data subject - e.g. to the collection of his medical data for an EHR and to any future transfers of these medical data to health professionals involved in treatment - would not constitute consent in the terms of Article 2(h) of the Directive*.

Moreover, WP 131 highlights that "*consent by the data subject (must be) based upon an appreciation and understanding of the facts and implications of an action. The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues, in particular those specified in Articles 10 and 11 of the Directive, such as the nature of the data processed, purposes of the processing, the recipients of possible transfers, and the rights of the data subject. This includes also an awareness of the consequences of not consenting to the processing in question*".

The WP 187 "Opinion 15/2011 on the definition of consent", Adopted on 13 July 2011, reports that "*The more complex data processing is, the more can be expected from the data controller. The more difficult it becomes for an average citizen to oversee and understand all the elements of the data processing, the larger the efforts should become for the data controller to demonstrate that consent was obtained based on specific, understandable information.*"

The Working Party stated that "*This Opinion is partly issued in response to a request from the Commission in the context of the ongoing review of the Data Protection Directive. It therefore contains recommendations for consideration in the review. Those recommendations include:"*

*(i) clarifying the meaning of "unambiguous" consent and explaining that only consent that is based on statements or actions to signify agreement constitutes valid consent;*

*(ii) requiring data controllers to put in place mechanisms to demonstrate consent (within a general accountability obligation);*

*(iii) adding an explicit requirement regarding the quality and accessibility of the information forming the basis for consent, and*

*(iv) a number of suggestions regarding minors and others lacking legal capacity*

Furthermore, WP 223, states that "*users must remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific*" and continues stating that "*Indeed, empowering individuals by keeping them informed, free and safe is the key to support trust and innovation, hence to success on these markets.*"

An example cited by WP on WP223 is the following:

"*A health-related device uses a small light to monitor how blood flows in veins, and to derive heartbeat information. The device includes another sensor that measures blood oxygen level but no information is available on this collection of data neither on the device nor on the user interface. Even if the blood oxygen sensor is fully functional, it should not be enabled without first informing the user. Explicit consent will be required to enable this sensor.*"

Taken into account all the considerations above reported, it is understandable the need of requirements clearly defined that will support data subjects and e-health professionals.

### 2.4.1 Issues Related to the "Consent"

Consent to process personal/sensitive data should be informed. However, this is sometimes very difficult because many IoT devices are not designed to facilitate information to interested users. There is therefore:

- The need to obtain prior and informed consent, unless the treatment is objectively necessary, i.e., for the execution of a contract to which the data subject is party. The notice must state the identity of all those involved in various ways in the processing of personal data and specify that "*data subjects must have a possibility to revoke any prior consent given to a specific data processing and to object to the processing of data relating to them*" (WP223) at any time.
- The need to store and process only data collected on the data subject "*strictly necessary for the specific purpose previously determined by the data controller (the "data minimisation" principle)*" (WP223).

## 2.5 Jurisdiction

The exclusive problem with Internet jurisdiction in IoT might be the presence of numerous parties in several parts of the world. Then, if one party wants to sue the other, where can he sue? Traditional requirements generally comprise two areas:

1. the Place where the defendant resides, or
2. where the cause of action arises.

At large, in the context of the Internet, considering the lack of physical boundaries, both these are difficult to establish with any certainty. For example, a single transaction (e.g. data processing) can involve the laws of three jurisdictions:

1. the laws of the state/nation in which the user resides,
2. the laws of the state/nation that apply where the server hosting the transaction (e.g. data processing) is located, and
3. the laws of the state/nation which apply to the person or business with whom the transaction (e.g. data processing) takes place.

So, a user in one of the Indian States conducting a transaction (e.g. data processing) with another user in Britain through a server in Canada could theoretically be subject to the laws of all three countries as they relate to the transaction at hand.

In any case, in the privacy context it's necessary to refer to the European regulation (Directive 95/46/CE) to find out which is the correct regulation to apply to the specific case.

# 3 Security and Privacy in a Real Scenario

Medical devices connected to the network may be beneficial in many ways (time and money saving, rapidity of intervention), but may also be over shadowed by several critical issues: the theft of personal information, intentional and malicious tampering devices, deterioration and accidental failures. Medical devices in the network, therefore, are vulnerable as any other related technology. When, through a device connected and plugged into a person, a computer crime is committed, it is not always easy to identify the person held responsible for the custody and preservation of data staff treated (also in terms of omission in the adoption of security measures and/or organizational measures for the protection of personal data).

Moreover, we should also consider attacks aimed at people with the intent to cause physical harm. This is the case of, for instance, implantable cardioverter defibrillators (ICD), pacemakers or even insulin pumps. The first two devices, so important to the health of millions of people suffering from heart disease, are not designed to withstand attacks. Indeed, both defibrillators and pacemakers can be reprogrammed, forcing them to shut down or send a potentially fatal electric shock, or even infect other pacemaker or ICD. Moreover, the use of wireless control systems, in fact, exposes at least a theoretical risk of intrusion, sabotage and even theft of sensitive information. The researchers have succeeded to collect personal data of some patients by capturing signals emitted by radio systems implanted.

It is essential, therefore, that the safety of these medical devices is integrated from the moment of their design, and not reconsidered at a later time, thus ensuring an approach secure by design (and, therefore, also privacy by design). The IoT, in fact, allows the creation of tools to detect and continuously monitor parameters essential to health, to be included in the "wearable technology": bracelets, clothing, sensors with functions related to health that operate even through smart phones. This allows a great development of telemedicine and home care, which are becoming increasingly innovative fields.

## 4 Conclusions

One of the main issues relating to security and privacy is the analysis of the data flow in a IoT architecture that should be designed in accordance with the new principles of "Privacy by Design" and "Privacy by default", and verified by PIA. Although the IoT implementation of security mechanisms and privacy has been widely debated [15], there is still the open question of who should be in charge of informing users about the management of their personal/sensitive data and to collect and store all consents. In particular, the "lack of control" on the data is one of the main issues to wonder about. In fact, the sharing of personal data among physicians, device manufacturers, software developers, suppliers of computing power, clouds providers and analysts, entails for the people whose data are processed, extremely difficult to exercise proper control over these data, the method of their transmission by IoT devices, shared between third parties and, above all, on the objectives pursued different from those associated with the device (so-called "secondary use"). As above reported, WP 223 states that "*users must remain in complete control of their personal data throughout the product life-cycle*". Thus, it remains to be clearly identified the role of all the actors in IoT (e.g. physicians, developers, IoT producers, etc.) in the management and storage of the collected data.

At the end of this analysis, we cannot provide a final answer to all poised questions, however, we may suggest technological and procedural efforts.

Standardizing requirements represent a mandatory issue that should ensure both uniformity in design research protocols and in strengthening digital privacy and security. This will be ensured one the one hand by providing the constructor with definite rules as to how to "maximize" the efforts to ensure adequate data protection and privacy ("Privacy by Design") and on the other by refining and reinforcing the regulations governing privacy and security. This point is of outmost interest when considering the perception that a general IT tool end-user has of the technology he/she is facing. Indeed, most people consider information stored on their mobile phones to be as or more protected than that stored in their personal computers (Urban et al. 2012), although it is virtually impossible to keep track of where data are being held, by whom, and for which purpose. Similarly, people consider data stored in institutions (such as online banks) to be safe and no one describes the potential dangers related to data breaches. This altered perception of privacy should hint new efforts at enhancing technological literacy of the population and at increasing public's knowledge of privacy and security in order to exercise a proper control over their data.

Likewise, in health research data protection depends on institutions, investigators and sponsors, although it appears unrealistic to think that ethical obligations can be fully met without guidance and resources. Also in this case, the governments should promote the development of education, certification, and accreditation systems that apply to all researchers, rather than mandating that privacy and confidentiality be "maximized" [The National Institutes of Health Guidelines for the Conduct of Research Involving Human Subjects (2004)]. In this way, the ethical obligation to protect participants, which lies first with researchers, can be more easily met, as requested by National Bioethics Advisory Commission (NBAC) (2001).

**Acknowledgements.** Partially supported by the ESF - Italian Ministry of Education, University & Research PON03PE_00146_1/10 BIBIOFAR (CUP B88F12000730005).

## References

1. Gershenfeld, N., Krikorian, R., Cohen, D.: The Internet of Things. Sci. Am. **291**, 76–81 (2004)
2. Granjal, J., Monteiro, E., Silva, J.: Security for the Internet of Things: a survey of existing protocols and open research issues. IEEE Commun. Surv. Tutor. **17**, 1294–1312 (2015)
3. Medaglia, C.M., Serbanati, A.: An overview of privacy and security issues in the Internet of Things. In: Giusto, D., Iera, A., Morabito, G., Atzori, L. (eds.) the Internet of Things. Springer, New York (2010). doi:10.1007/978-1-4419-1674-7_38
4. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2014/wp223_en.pdf
5. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf
6. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf
7. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2014/wp216_en.pdf
8. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf
9. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf
10. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2011/wp187_en.pdf
11. http://ec.europa.eu/justice/data-protection/index_en.htm
12. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//IT
13. Dong, C., Guiran, C., Lizhong, J., Xiaodong, R., Jiajia, L., Fengyun, L.: A novel secure architecture for the Internet of Things. In: Proceedings of 2011 Fifth International Conference on Genetic and Evolutionary Computing (ICGEC) (2011)
14. Alcaide, A., Palomar, E., Montero-Castillo, J., Ribagorda, A.: Anonymous authentication for privacy-preserving IoT target-driven applications. Comput. Secur. **37**, 111–123 (2013)
15. Fan, W., Bifet, A.: Mining big data: current status, and forecast to the future. SIGKDD Explor. Newsl. **14**, 1–5 (2013)
16. Steele, R., Clarke, A.: The Internet of Things and next-generation public health information systems. Commun. Netw. **5**(03), 4 (2013)