Author: Tim Sandle

Published on IVT Network (www.ivtnetwork.com)

GXP Volume 24, Issue 3 – May 2020

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

APPLICATION OF WIRELESS TECHNOLOGY IN THE PHARMACEUTICALS SECTOR: MAINTAINING DATA INTEGRITY, SECURITY AND PRIVACY

INTRODUCTION

The pharmaceutical manufacturing facilities of today are beginning to look different to those even from five years ago. Innovations include the use of modular construction platforms, new single-use process equipment, contained process equipment, and digital technology. Each innovation has its own rationale, with many designed to increase flexibility and reliability, and to lower capital costs and maintenance costs. This article looks at one aspect of digital technology: the importance of data handling though the increased use of Wi-Fi.

The applications of wireless technology in pharmaceuticals are broad ranging and include collecting data from process instruments; controlling actuators; undertaking equipment diagnostic and condition monitoring; assessing the process environment, through the use of sensors; airborne particle counting; and enabling moveable and reconfigurable equipment, allowing for the creation of more flexible process areas and laboratory environments.

Data collected from the pharmaceutical plant can be held on computerized systems, servers or portable media; it can also be traveling through wired or wireless networks. At any location, data is always at risk from intentional and unintentional breaches, together with problems arising from intermittent connections, lost data, and security risks. In addition, problems can arise due to inappropriate selection of technology or with poor configuration, such as:

- Poorly characterized or poorly utilized wireless systems (e.g., wireless networks).
- Lost, corrupted, or time-delayed transmissions, and degradations in wireless transmissions including when caused by competing wireless signals or electromagnetic interference affecting wireless transmissions.

In the article, some of the general risks in relation to data security, cyberattacks, data privacy, signal disruption, and data integrity are considered, alongside the specific risks that come with the application of Wi-Fi. For the most part these risks can be mitigated, provided appropriate protocols are adhered to enabling the benefits of Wi-Fi to be realized. This is not an overly technical article in terms of explaining the intricacies of wireless technology; the attention is to outline the main challenges and concerns to draw out those issues pertinent to a wireless technology digital strategy for the pharmaceutical organization.

Wi-Fi

Wi-Fi (wireless fidelity, sometimes written as WiFi) refers to the application of short-range wireless transmission technology, which enables signals to be sent up to hundreds of metres away in order to support access to the Internet and for creating a local area network (generally referred to as a WLAN (Wireless Local Area Network or WLAN) (1). The design of the technology is based on IEEE 802.11 family of standards (which are operated by the Institute of Electrical and Electronics Engineers (IEEE); in fact, Wi-Fi is the colloquial name for 802.11) (2). Different generations of Wi-Fi as represented by letters after standard reference ‘802.11’. With Wi-Fi, there are two main devices required: a wireless client and an access point (router), which provides the radio signals to connect to the Internet. This is a different format for data transfer compared with a wired service, which uses ethernet (3). Data transfer is he process of moving data between one or more nodes. Digital data transfer converts data into digital bit streams.

Wi-Fi speeds vary with the particular generation of Wi-Fi in use; Wi-Fi equipment with the 802.11ac standard can achieve speeds up to gigabits per second. In terms of range, radio signals grow weaker as the distance between the transmitter and receiver increases; the maximum distance for Wi-Fi also depends on the standard, with 802.11a allowing 29 meters (95 feet) and 802.11n topping out at 70 meters (230 feet). Outside this range, Wi-Fi may not work at all. Wi-Fi systems differ in the way that a signal is sent (the manner in which data signals travel through a radio frequency). The two main systems are narrowband, where data travels straight through a single radio frequency band; and spread spectrum, where data signals either alternate between carrier frequencies or constantly change their data pattern. Spread spectrum is superior, designed to trade bandwidth efficiency for reliability, integrity, and security.

Signals can also be impacted or blocked by walls, equipment and other items which can interfere with and scatter radio signals, compromising the speed of wireless networks. The material of composition is also a factor, with non-metallic objects tending to absorb radio energy, reducing signal strength; and metal objects reflecting radio waves, creating “dead spots” in certain areas. Interference can also occur from other devices. Wireless technologies, such as 802.11b/g, use a radio frequency range of 2.4GHz, as do many other devices, such as smartphones. Devices that share the channel can cause noise and weaken the signals. Electrical interference can arise from devices such as computers, lighting fixtures, or from different motorized devices. Types of electrical interference include electromagnetic disturbances, such as radiated and conducted emissions; and electrostatic discharge.

The impact that electrical interference has on the signal depends on the proximity of the electrical device to the wireless access point. These issues mean that real-world Wi-Fi data transfer rates are typically only a fraction of the maximum possible speed; changing the location of devices can help to improve wireless network communications.

Many industries are investing in wireless technology and are using Wi-Fi networks in order to increase connectivity and the speed of data collection and analysis. From early warnings, to big data analytics, and with real-time monitoring, there are many advantages that are helping to propel industrial wireless adoption. Other advantages include reliability and ease of implementation, such as being able to install wireless devices without any significant disruption to operations. In relation to fitting, the installation costs are often relatively lower compared with wired solutions since cabling is not necessary (moreover, expanding data capture coverage for new equipment, or with moving equipment in a new location, or when enlarging a cleanroom using a wired solution requires construction works, drilling, pulling wires and so on, which is highly disruptive and very expensive). With the issue of reliability, many devices operating across wireless networks have self-contained power sources that can operate for years without the need for replacement.

In discussing some of the Wi-Fi and data control associated issues with the pharmaceutical sector, it should be noted that there are alternative technologies to Wi-Fi, including those that are wired (as with ethernet) and wireless (such as Bluetooth, cellular networks, and WiMax). These alternatives will also be subject to the same data security and integrity concerns. With these technologies: Bluetooth (over IEEE 802.15.1), ultra-wideband (UWB, over IEEE 802.15.3), ZigBee (over IEEE 802.15.4), and Wi-Fi (over IEEE 802.11) are four protocol standards for short- range wireless communications with low power consumption. From an application point of view, Bluetooth is intended for a cordless mouse, keyboard, and hands-free headset, UWB is oriented to high-bandwidth multimedia links, ZigBee is designed for reliable wirelessly networked monitoring and control networks, while Wi-Fi is directed at computer-to-computer connections as an extension or substitution of cabled networks. The focus in this article is with Wi-Fi technology.

When selecting Wi-Fi technology, as part of the user requirement specification, the pharmaceutical organization should define (4):

- The specific radio frequency wireless technology type (e.g., IEEE 802.11b).
- The characteristics of the modulation
- The type of radiated radio frequency power.

- Specification of each radio frequency frequency or frequency band of transmission and the preferred frequency or frequency band.
- Specification of the bandwidth of the receiving section of the equipment or system in those bands.
- Functions and performance of the wireless data transmissions including data throughput, latency, and data integrity.
- Information about any limitations on the number, output power, or proximity of other in-band transmitters used in the vicinity that might adversely impact a device's system operation.

Application of wireless technology in the pharmaceutical facility

Wireless technology is becoming more commonplace in the pharmaceutical facility, with data transmitted over Wi-Fi networks, supported standalone or connected devices (with several devices coming together to create an Industrial Internet of Things). Many applications involve the deployment of wireless sensor networks. These networks consist of the smallest unit of a network that has the required features (5). The use of several sensors supports large scale deployment, mobility, and reliability. The sensor network consists of a discrete group of independent nodes that communicate wirelessly over limited frequencies at low bandwidth area. Sensors can be used to collect the environmental data (such as temperature, humidity, mixing speed and so on) and transmit the data to the base station or remote location. At a later stage, and sometimes in real-time, the raw data is processed for detailed analysis at the remote server according to the application requirements.

Examples of application include the use of wireless mobile particle counters, that can be made into areas and moved around so that benefits from greater portability can be realized. This portability is especially useful when undertaking an exercise like cleanroom classification.

A second example is with the assessment of steam trap performance from within the plant room, a task generally carried out by maintenance personnel, assessing whether water is being expelled at normal rates and there is no plume of live steam. This task can be automated through the use of portable acoustic device that can monitor the characteristic sounds of a properly operating mechanism continuously and send alarms using wireless technology for when the acoustic signals show atypical variation.

A third application is with high-precision flowmeters. These are devices that can assist with assessing different manufacturing processes, such as wash-down applications. Such devices can help to monitor for process reliability, and they can also be used to avoid excessive water usage, thereby playing a role in cost control.

A fourth concept is with process control, such as the use of temperature sensors fitted to measure the contents of a reactor, where data can be wirelessly sent to a host system controlling the reactor, and necessary adjustments made should the temperature begin to increase or decrease outside of the expected values (6).

A fifth aspect is with portability, applied to both the production and laboratory setting. At times equipment needs to be moved as areas are expanded or redesigned. Moving reactors, freezers and other equipment is often challenging, under change control and often requiring repeat temperature mapping. This process becomes even more difficult when wired connections must be re-established in a different area; this is something avoided with wireless technology. A sixth example is with cold-chain data loggers, where data is transmitted wirelessly and informs about the transport or storage conditions to which a pharmaceutical product has been subjected to. A related application (example eight) is with the use of dataloggers for thermal mapping sterilization devices like autoclaves. A ninth example is with glove integrity leak testers for isolators, where information about the robustness of an isolator gauntlet can be sent via WLAN (7).

A tenth area is with medical devices, including those intended to monitor patient vital signs in the home setting. The incorporation of wireless technology in medical devices can deliver several benefits, such as increased patient mobility (through the removal of wires) and providing medical professionals with the ability to remotely program devices, and providing a stream of data to clinicians, which can be accessed remotely, to monitor patient health outside of the clinical setting. Pharmaceutical companies also collect data from devices, such as smart inhalers, signalling further advances with medical technology (a matter that introduces privacy concerns, as considered below).

The above section demonstrates some of the advantages that can potentially be gained from the adoption of wireless technology in the pharmaceutical setting. There are, however, some concerns that need to be considered in relation to data security and data integrity.

Concerns in relation to wireless deployment in pharmaceuticals

There are an array of concerns, complexities and challenges in relation to the deployment of wireless technology within the pharmaceutical facility. Challenges include reliable data transmission, node mobility support and fast event detection, timely delivery of data, power management, node computation and configuring middleware. Furthermore, there are issue pertaining to data security, data integrity, and data privacy.

Many of the concerns relate to the vulnerability of data in transit. As data is transmitted, say between a sensor and receiver, then the wireless communication ranges are not confined, and hence they are vulnerable. As data is being sent (in transit), it is at risk from loss of integrity or from being attacked. In terms of cybersecurity risks, attacks can occur via data interception, where device data is compromised (such as breaking a cryptographic key); and message modification, where data is intercepted and tampered with. Other cybersecurity concerns are discussed below.

To assess data transit, the wireless network needs to be qualified. Data validation is the process of comparing data with a set of rules or values to find out if the data is correct. Many programs perform a validity check that analyze data; or, a manual system is required. Such an exercise will need to be run on more than one occasion, in order to assess data consistency and usability.

Wireless concern #1: Data security

The greater expansion of connected devices brings with it a new set of cybersecurity concerns. A cyberattack on a Wi-Fi network generally falls into one of two groups

- On network access control, data confidentiality and data integrity protection.
- On wireless communication network design, deployment, and maintenance.

Both forms of attack are possible where there are weaknesses in wireless security protocols. Such protocols are primarily used for data encryption, maintaining confidentiality, data integrity, and for verifying the authenticity of packets or data. There are three main wireless protocols used:

- WEP (Wired Equivalency Privacy) + RC42.
- WPA (Wi-Fi Protected Access) +TKIP3.
- WPA2(Wi-Fi Protected Access Version 2) +AES

With these protocols, WEP was the original and it is the weakest type of protocol since it enables hackers to easily forge authentication messages. WPA was designed with aim of addressing WEP cryptography weaknesses. The standard WPA is designed for small office and home/domestic use, where authentication does not use an authentication server and the data cryptography key is only formed of 256 bits (an alphanumeric string). This form is not suitable for the pharmaceutical sector. The second form is Enterprise WPA, where authentication is created by an authentication server 802.1x, generating better control and security across the wireless network (8).

Backing-up the data is key to good security practices, ideally onto a separate server or onto the cloud (which offers advantages of portability and brings with it additional security concerns). In terms of frequency of back-ups, this needs to regular balanced against the time, cost and any performance issues which occur whilst the back-up process is taking place.

Other security measures include automatic log off functionality. With this, logging off a user with after each session will terminate the session cookie, cutting off access to the attacker if he somehow manages to intercept it. Further good practices include:

- Putting in place protection against unauthorized wireless access to device data and control. This should include protocols that maintain the security of the communications while avoiding known shortcomings of existing older protocols (such as Wired Equivalent Privacy (WEP)).
- Ensuring there are software protections for control of the wireless data transmission and protection against unauthorized access.

Security measures can be assessed through running tests and conducting audits. A common test, requested by larger companies, is a penetration test where an authorized attempt is made to hack into a system, sometimes employing the efforts of an external ‘ethical’ hacker. Security audits tend to be conducted internally by a data integrity specialist. A cybersecurity audit should analyse:

- Employee security practices.
- What information is mission-critical for an organization.
- Potential methods a hacker might employ to get his hands on the information.
- What security procedures are in place to identify a potential hacking.

More specific issues relating to cybersecurity are discussed below.

Wireless concern #2: Data integrity

Data integrity refers to maintaining and assuring the accuracy and consistency of data over its entire lifecycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data. Data integrity is a key regulatory concern, as set out in guidance documents which have been produced by the U.S. Food and Drug Administration (FDA) (9) and the MHRA (10). Hence, data integrity is of great importance to the pharmaceutical sector, and there is a requirement to demonstrate that all data collected is reliable and valid. The broad principles of data integrity have been covered in other articles (for definitions of ALCOA - Attributable, Legible, Contemporaneous, Original and Accurate for data – and related aspects) (11); the focus here is with specific data integrity issues which can affect wireless networks.

Data integrity principles across a network relates to the overall completeness, accuracy and consistency of data, applying similar principles to other aspects of data management within the pharmaceutical sector. Data integrity must be verified when sending data through a network, and this includes the use of error checking and correction protocols. Such protocols verify that the data collected and sent is the same as the data received.

For wireless technology, there are three dimensions to data integrity:

- Secure communication: Verifying the information has been correctly and securely sent from the creator, to the receiver.

- Safe storage: Verifying the data that is in servers has not been altered or modified and can still be used for its original purposes.
- Data can be audited: Verifying data at each point where changes were made, allowing for modifications and other alterations to be detected.

Data integrity issues can arise through:

- Human error, whether malicious or unintentional.
- Transfer errors, including unintended alterations or data compromise during transfer from one device to another.
- Bugs, viruses/malware, hacking, and other cyber threats.
- Compromised hardware, such as a device or disk crash.
- Physical compromise to devices.

To safeguard the wireless network, there should be multi-level password control; user access rights which prevent data amendments; measures to prevent user access to clocks; having automated data capture; ensuring systems have data backup; and ensuring that an audit trail is in place and subject to regular checks.

Other data integrity considerations for a wireless network include noting any limitations or restrictions for proper operation and radio frequency wireless performance (e.g., alarms, back-up functions, alternative modes of operation) when the radio frequency wireless link is lost or corrupted.

In terms of qualifying a wireless network, it must be confirmed that the captured data is fully transferred and that the receive data is identical, with no indication that these data have been altered or corrupted (12).

Where errors occur, this is sometimes referred to as ‘dirty data’. Forms of such data include:

- Misleading data
- Duplicate data
- Incorrect data
- Inaccurate data
- Non-integrated data
- Data that violates business rules
- Data without a generalized formatting
- Incorrectly punctuated or spelled data

As well as technical errors, data can be affected by cyberattacks, as discussed above.

When assessing Wi-Fi for data integrity considerations, the user should be in a position to answer the following questions:

1. Is electronic data available?
2. Is electronic data reviewed?
3. Is meta data (audit trails) reviewed regularly?
4. Is there clear segregation of duties?
5. Has the system been validated for its intended use?

A satisfactory answer should be available for each of these five key questions, in order to a wireless system to be accepted.

Wireless concern #3: Cyberattacks

As with other parts of the Internet, WiFi is open to attacks from malicious hackers who seek to exploit software and security vulnerabilities. The biggest security vulnerability remains weak passwords. Weak passwords can be addressed by the password configuration requiring a variety of numbers and symbols, although any password management needs to be supported by employee education. This will include things like not sharing passwords or other personal identifiable information between employees. This prevents employees with attribution in one field (such as quality assurance) to access and modify data from colleagues in unrelated fields (such as production).

A second area of vulnerability with people arises from employees falling for phishing scams and other forms malicious attack, designed to trick people into clicking onto a malicious link which allows malware to enter onto a network. It is good practice for employees to remain vigilant in terms of looking for signs of hacking, such as unexpected changes to passwords, missing files, logins at strange hours, file modifications that cannot be accounted for, and so forth.

A third vulnerability exists when data has not been encrypted. Encryption information means that the person in receipt of the data cannot access that data without the use of a decryption key. While this process is effective, a risk exists should a hacker acquires the files stored on the database or obtains the decryption key or manages some other means to encrypt the data with their own encryption process. It is important that Wi-Fi networks are encrypted; errors can arise from the standard settings, where Wi-Fi access points typically default to an encryption-free (open) mode and will remain open unless configured otherwise (13). The creation of Virtual Private Networks can be used to improve the confidentiality of data carried through Wi-Fi networks, in contrast to the risks associated with public Wi-Fi networks. A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. This is a useful consideration since many companies will have pubic spaces where Wi-Fi can be accessed (such as for visitors), close to where sensitive data is being captured and transmitted.

A fourth area of concern is with metadata, such as: date of last file modification, the author of the modifications and general description of data. A person of malicious intent may be interested in metadata in order to obtain information about the operating systems the organization uses, which provides the hacker with the background for selecting a with a particular exploit kit (similar exploitation can occur if information is obtained about application-specific data). Furthermore, obtaining information like email addresses enables the hacker to conduct phishing attacks. Depending on the configuration, an attack on metadata can lead to usernames and passwords being exposed. One may through which metadata is often obtained is through obtaining documents (like PDF files), which can be scanned, and metadata extracted.

A fifth area of concern is through physical access to a system, such as the use of USB sticks which can be used to collect data, and which are invariably unsecure. USB sticks can also inadvertently put malware onto a network.

A sixth area arises due to coding errors. An example of bad code is with buffer overflows. Poor configurations can additionally present an attacker with the opportunity to deploy brute-force login screens, and through this acquire user passwords.

A seventh area of concern arises as a result of system volume and stress in relation to databases. This also places systems at risk from cyberattacks (as discussed below), where some technical attacks occur because the hardware itself cannot cope with the amount of information it has to process.

An eighth issue is with denial-of-service attacks. This form of cyberattack prevent a wireless network from operating, where an attacker attempts to disrupt the network's operation by broadcasting high-energy signals. In situations where the broadcasting is powerful enough, then the entire network communication can become jammed. Similar types of attacks include delaying communication by violating the medium access control protocol or causing wireless disruption by transmitting data packets while a neighbour node is also transmitting (14).

A ninth area impacts sensor devices manufactured by pharmaceutical companies for patient monitoring, such as wearable sensors. One risk here is a threat to patient privacy from eavesdropping, such as unauthorised access to patient vital sign snooping, where patient information is collected from wireless communication channels. Such personal identifiable information can additionally include location, timestamps, source address, destination address as well as the actual vital signs data (15).

Some organizations adopt threat vulnerability checklists to assess potential weaknesses and cybersecurity concerns. This can be enhanced by risk scoring, such as high risk, low risk, or no risk. For example (16):

- Attack Vector (physical, local, adjacent, network).
- Attack Complexity (high, low).
- Privileges Required (none, low, high).
- User Interaction (none, required).
- Scope (changed, unchanged).
- Confidentiality Impact (high, low, none).
- Integrity Impact (none, low, high).
- Availability Impact (high, low, none).
- Exploit Code Maturity (high, functional, proof-of-concept, unproven).
- Remediation Level (unavailable, work-around, temporary fix, official fix, not defined).
- Report Confidence (confirmed, reasonable, unknown, not defined).

Once such a task is completed and risks addressed, the process of 'cyber hygiene' should be adopted including the reassessment of risk assessments, and with proactively seeking opportunities to reduce cybersecurity risks even when residual risk is acceptable.

In terms of on-going assessments of data integrity as impacted by cybersecurity, as well as a security audit (outlined above), audit trails should be regularly assessed as part of the data integrity measures. The audit log tracks the creation, deletion and modification of each electronic record, and with this every action is time stamped. Hence, reviewing the audit trail allows for the reconstruction of all the steps taken to obtain a certain result. This not only helps to assess the reliability of data it can also assist with pinpointing a security breach. Audit trails should be automatically generated and configured in such a way so that the user does not have the capability to alter or to update the audit trail.

Wireless concern #4: Disruption of data signals

The ability of a system to continually transmit data at all times is an important concern, such as with the earlier discussion concerning signal interference (something that is likely to increase as the Internet of Things expands since all wireless technologies face challenges by coexisting in the same space). Before adopting wireless technology, it is good practice to run a simulation of the system to assess if there is a suitable facility within the facility. This is something that will become more challenging if remote equipment is to be used. This can be assessed by placing a sensor in one location and seeing if a computer, with the appropriate data capture and analytical software can collect the data. This should be assessed in real-time and over a sufficiently long period of time, such as 24 hours, to determine if any communication failures are detected (17).

Wireless concern #5: Data privacy

Data privacy and confidentiality may affect some systems in use at the pharmaceutical facility, outside of systems operated by human resources. This can include the recording of video images from remote cameras to assess pharmaceutical processing and door entry logs. Whilst Good Manufacturing Practices permits data to be collected and used for batch release, attention should be paid to regional, national and supranational data privacy laws and the regulatory risks should data go missing or be obtained by an unauthorised third party. An additional set of concerns arise for pharmaceutical companies who develop devices for the monitoring of patient health, where the collection of data held needs to meet strict legal and ethical obligations of confidentiality. These health data should be confidential and available only to the authorized medical professionals.

Pharmaceutical companies developing sensor devices need to be mindful of patient rights. Appropriate questions to consider are (18):

- Who can have permission to own the data?
- What type of medical data, how much, and where should the data be collected?
- Who can have permission to inspect the medical data?
- Whom should medical data be revealed to without the patient’s consent?

Patients should have the rights to determine which data should be collected, used or disclosed, under legislation like the U.S. National Committee for Vital and Health Statistics (19) and European Union Data Protection Directive (20).

RISK ASSESSMENT

Each of the concerns should be assessed through the use of risk assessment. An example is with the use of threat modelling, which is a methodology for optimizing wireless security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system (21). This approach can strengthen security by identifying vulnerabilities and threats to a particular system and to consider data integrity vulnerabilities.

CONCLUSION

This article has considered the advantages that wireless technology can offer pharmaceutical and healthcare companies. In presenting some examples of application, the article has focused on key concerns such as data security and data integrity. With data integrity, it is important that the user of any wireless network can guarantee at the recipient end that the data has not been altered in transit. Both data security and data integrity for wireless networks are interrelated terms; data security refers to the protection of data against unauthorized access or corruption and is necessary to ensure data integrity; and data integrity is a desired result of data security, and both are equally important. A third dimension is with data privacy, which is applicable internal to the organization and in relation to devices designed to collect patient data and to transmit data wirelessly.

In summary, the focus with wireless networks should be that:

- Data remains confidential.
- Data cannot be modified.
- Data cannot be replayed.
- Data corruption and loss of integrity can be detected.

Author: Tim Sandle

Published on IVT Network (www.ivtnetwork.com)

GXP Volume 24, Issue 3 – May 2020

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an **informa** business

While wireless technology and Wi-Fi networks can confer many advantages to pharmaceutical companies, considerable effort needs to be put into the digital strategy in order to ensure data is secure, integral and that privacy, as required, is maintained.

REFERENCES

1. Aime, Marco; Calandriello, Giorgio; Lioy, Antonio (2007). Dependability in Wireless Networks: Can We Rely on WiFi?, *IEEE Security and Privacy Magazine*. 5 (1): 23–29. doi:10.1109/MSP.2007.4
2. Banerji, Sourangsu; Chowdhury, Rahul Singha. (2013) On IEEE 802.11: Wireless LAN Technology. *International Journal of Mobile Network Communications & Telematics (IJMNCT)*, 3 (4): arXiv:1307.2661
3. Shoch, J. F. Dalal, Y. K., Redell, D.D., and Crane, R.C. (1982). Evolution of the Ethernet Local Computer Network, *IEEE Computer*. 15 (8): 14–26. doi:10.1109/MC.1982.1654107.
4. FDA (2013) Radio Frequency Wireless Technology in Medical Devices, U.S. Department of Health and Human Services Food and Drug Administration Center for Devices and Radiological Health. At: https://www.fda.gov/media/71975/download (accessed 11th February 2020)
5. Ko B.J.G., Lu C., Srivastva M.B., Stankovic J.A., Terzis A., Welsh M. (2010) Wireless Sensor Network for Healthcare. *Proc. IEEE*. 98:1947–1960
6. Yang, Z.P., Huang, Q.Z., Wang, M. (2014) Study on application of wireless sensor networks in military highway transportation battlefield environment. *Equip. Environ. Eng*. 11(03), 78–82
7. Appel, K. (2011) Pharmaceutical Distribution: Monitoring for Compliance and Risk [online]. *MHD Supply Chain Solutions*, 41 (2): 70-74
8. YongJian, F., Hong, C., Ying, Z.X. (2012) Data privacy preservation in wireless sensor networks. Chin. J. Comput. 35(6), 1131–1146
9. FDA (2016) Data Integrity and Compliance With CGMP, Draft Guidance for Industry, April 2016, U.S. Department of Health and Human Services, Food and Drug Administration, Washington
10. MHRA (2015) MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015, Medicines Healthcare products and Regulatory Agency, London, UK
11. Sandle, T. (2016) Data Integrity Considerations for the Pharmaceutical Microbiology Laboratory, Journal of GXP Compliance, 20 (6): 1-12
12. Sang, Y., Shen, H., Inoguchi, Y., Tan, Y., Xiong, N. (2006) Secure data aggregation in wireless sensor networks: a survey. *2006 Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies*, pp. 315–320
13. Le X.H., Khalid M., Sankar R., Lee S. (2011) An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Network in Healthcare. *J. Networks*. 27:355–364
14. Raymond D.R., Midkiff S.F. (2008) Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervas. Comput*. 7:74–81
15. Dimitriou T., Loannis K. (2008) Security Issues in Biomedical Wireless Sensor Networks. *Proceedings of 1st International Symposium on Applied Sciences on Biomedical and Communication Technologies* (ISABEL'08); Aalborg, Denmark. 25–28 October 2008
16. FDA (2014) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, U.S. Department of Health and Human Services Food and Drug Administration. At: https://www.fda.gov/media/86174/download (accessed 10th February 2020)
17. Loof, T. (undated) Wireless Particle Monitoring of Pharmaceutical Cleanrooms, Particle Measuring Systems whitepaper. At: http://www.pct.hu/wsp_images/wireless_pharma_app76.pdf (accessed 10th February 2020)
18. Meingast M., Roosta T., Sastry S. (2006) Security and Privacy Issues with Healthcare Information Technology. Proceedings of the *28th IEEE EMBS Annual International Conference*; New York, NY, USA. 31 August–3 September 2006; pp. 5453–5458
19. National Committee on Vital and Health Statistics Available online: http://www.ncvhs.hhs.gov/privrecs.htm (accessed on 7th February 2020).

20. The Data Protection Directive. EU Directive 95/46/EC. Available online: http://www.dataprotection.ie/viewdoc.asp?m=&fn=/documents/legal/6aii-1c.htm#1 (accessed on 7th February 2020).
21. Desmet L., Jacobs B., Piessens F., Joosen W. (2005) Threat Modelling for Web Services Based Web Applications. In: Chadwick D., Preneel B. (eds) *Communications and Multimedia Security*. IFIP — The International Federation for Information Processing, vol 175. Springer, Boston, MA