Handling electronic health data – main security and privacy guidelines

Theodor Adam, Florin Andrei, Larisa Gabudeanu, Victor Rotaru

In last decades, medical entities, such as hospitals, clinics, individual doctor offices (either public or private) have been collecting, processing and transferring more and more data about patients. Further, given that patients usually visit multiple medical entities for the same medical issue or for multiple medical issues throughout their lifetime, the issue of data security and privacy for the transfer of data arises.

Firstly, the manner in which the data by medical entities to patients has evolved from paper to electronic formats (the reverse data flow from patient to doctors is also applicable). Secondly, in certain cases data is transferred within the same medical entity or towards another medical entity. For example, the second opinion market that has been growing in recent years would benefit from a swifter manner of centralizing all data about a patient in one location and obtaining data in a centralized manner for review. Each of these data flows has specific privacy and security aspects to have in mind.

This article analyses these types of data flows and provides insight into the main privacy and security principles to be had in mind when designing such data flows and also approaches that may be taken in case of legacy systems already being set in place.

Consequently, the aim of this article is to outline the main security and privacy aspects to take into account for medical entities within their IT perimeter and when sending data to third parties (other medical entities, patients, specific doctors).

This article does not cover transfer of data to or from authorities or otherwise provided by law, such as the electronic patient records held by relevant authorities, clinical trials data handling or prescription handling. Further, the article does not cover the data collected, stored and otherwise handled by medical devices (which was detailed in https://cert.ro/vezi/document/medical-devices-how-to-secure) or implementation of telemedicine (which will be detailed in a subsequent article).

1. Know your data flows

As in any cases involving security, IT governance or data protection, the first step in setting-up proper internal infrastructure in line also with security and privacy requirements is to know where the data is stored and how it travels throughout your organization and towards third parties.

This may be difficult to maintain in case of large organizations. The first steps towards having this data flow map updated is the organizational culture towards security and privacy, but also a risk-based approach in which the main business processes are mapped to the IT resources used to support them. Of course, shadow IT is also of concern in this case and manners of mitigating it should be taken before this mapping takes place and also afterwards.

For completeness of the analysis, the locations where scanned copies of documents containing patient data is also required in order to properly secure these as well.

The main steps at this stage are as follows and represent the preparatory work before implementing the proposals in the following sections:

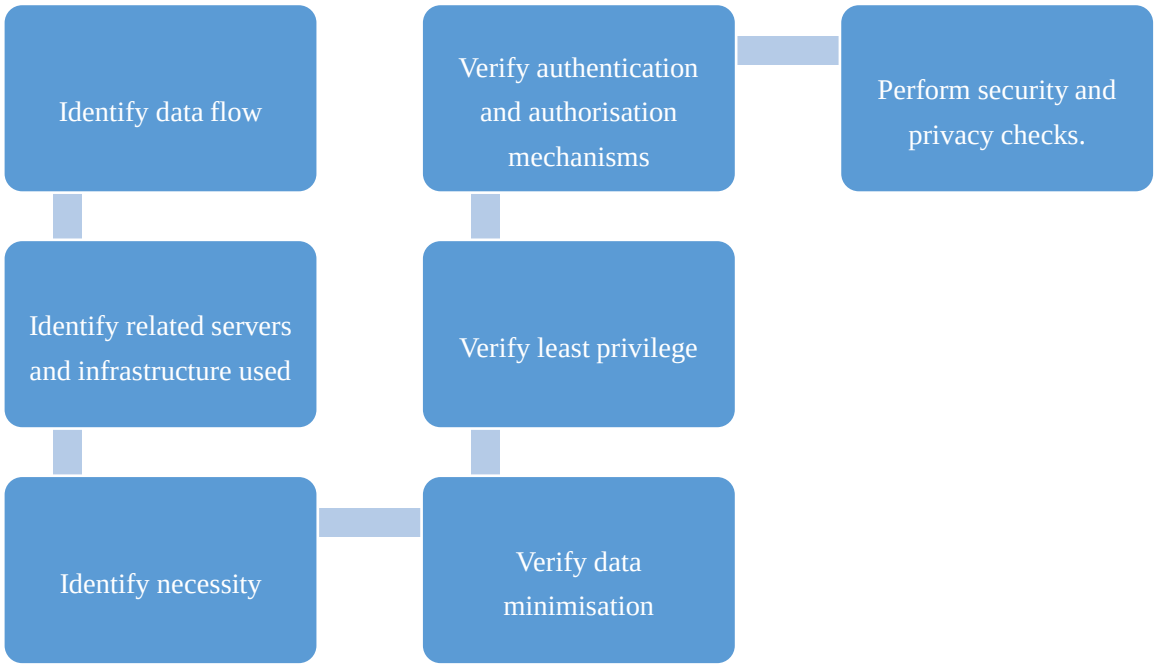

Figure 1 – Pre-design phase – identify data flows

Once these data flows are identified, an assessment of the business owner has to be made with respect to the necessity of these being in place.

Further, the interactions with third parties outside of the organization (patients, other medical organizations) should be identified in order to analyses further the manner in which the data is sent and accessed from a security and privacy perspective.

In addition, the internal data flows between various departments is relevant in order to identify the need to know requirements for accessing data and in order to ensure identity of identifiers used for patients, medical tests performed.

Whenever third parties are used for data storing, maintenance of IT systems holding data or data handling on behalf of the healthcare organization (defined as data processor under data protection legislation):

- proper contract have to be in place concerning the data to which they have access, including from a data protection legislation perspective;
- implementation of data minimization and need to know principles;
- retention periods and deletion triggers are established and implemented;
- ensuring that any transfer of data outside the EU (to a country without an adequate level of protection of personal data) complies with data protection legislation;
- third party warrants for and undertakes to hold proper security measures, audit or monitor the implementation of such security measures;
- the third party undertakes to replicate all of the above requirements with any of its sub-contractors.

Whenever data is sent to third parties holding or analyzing it on their own behalf, defined as data controllers under data protection legislation (e.g. for other healthcare services offered to the patient, for clinical trials):

- adequacy of basis for transferring should be analyzed and confirmed;
- transferring only the data needed under the identified transferring basis, thus implementing the data minimization principle;
- adequacy of transferring data outside the EU (to a country without an adequate level of protection of personal data), if this transfer occurs;
- proper information of individuals whose personal data is being transferred (e.g. patients) about the data transfer.

2. Communication between systems within the same organization

Healthcare organizations can have multiple departments that needs to be interconnected in certain situations – e.g. a patient is transferred from one department to another.

This transfer of data can be done in multiple manners and it definitely depends on the legacy systems in place within the healthcare organization. Some organizations use share drive, some have use paper, some use email and some have a centralized IT system.

Whereas we can build security on top of each of these to some extent, the preferred solution from an efficiency, time costs on the long run and limitation of organizational risks

(e.g. sending data to the wrong recipient or losing data) is the centralized IT system (or interconnection of existing IT systems within each department).

For this centralized IT system, the access management principles in the below sections are essential, which also entail proper management of user creation and deletion.

Aside from the data access, the main point to consider is the identification of a patient within all departments alike. This can be done by using a unique identifier for that patient, either unique within the hospital or uniquely issued by state authorities.

Especially for paper using organizations, the proposed solution, aside from enhanced security of the data, can ensure also proper accuracy of data, as data will not need to be re-typed in a different IT system and proper identification of medical tests and patients can be performed much easier.

In terms of access rights, of course, each department has to have access only to its patients and only to the data needed for their purpose. For example, the cardiology department may need access to the entire medical record of a patient transferred from the internal medicine department, as it needs to know all medical issues to avoid prescription of medicine that can affect the patient's health. However, the laboratory that needs to process a test may need access only to a limited amount of data in order to identify the patient for which the medical test is performed.

These type of intricate access rights may seem complex to design, but, generally, from the data flow mentioned above the need for data access should be clear and, if additional situations appear, a specific one-off transfer permission with choosing data to be transferred may be implemented.

If clinical trials are conducted within the healthcare organization, separate IT systems, interconnected or not with the healthcare organization ones should be contemplated, as this represents a distinct data processing activity than the general healthcare service providing.

3. Communication with patients

There are many ways in which communication with patients can be implemented. The method we are proposing in this article involves a designated space for communicating.

A designated space can be created for each patient or for each medical test taken by a patient. The model chosen depends on the needs of the healthcare organization.

Account per medical test: For organizations that offer patients medical tests, the approach with one user account per medical test may be easier to implemented and more secure. It is easier to implement because patients may come at various times for various medical tests and the user accounts can be generated at each interaction separately and automatically, with username and passwords that can be communicated to the patient when the medical test is taken. Having a single user account for all medical test in this case, where there is no constant

relation between the patient and the healthcare organization, may result in authentication issues, such as forgetting passwords and requesting password resets over the phone, potential unauthorized access to the account, higher degree of risk of unauthorized access to the account from having all health data (which is sensitive data under the data protection legislation) in a centralized location easily accessible to users outside of the healthcare organization.

For this situation, an ID of the user (e.g. patient ID) and an ID of the medical test can be provided to the patient when the medical test is taken.

Account per patient or patient visit: For organizations that have a constant relation with a patient (e.g. long terms monitoring of the patient due to a disease) and need for the patient to have at hand all of his/her medical records, it may be easier, from an organizational perspective, to have all the patient data (and test results) in a single user account.

Another hybrid option is to have, for instance, an account per patient visit. Thus, is a patient is committed to the hospital for a week, all of the relevant data pertaining to this period is stored in a separate account. Then, if the patient comes with a different medical issue two years later, a distinct account is created for this patient visit.

For this situation, a patient user ID can be setup when the account is first created and the password can be chosen then by the patient.

Further, in both use cases, the SCA (strong customer authentication) mechanism should be had in mind, with at least two out of the following three information being requested for authentication: knowledge (something only the patient knows – CNP, date of the medical test, ID of the medical test), possession (something only the patient possesses – an ID given by the healthcare organization) and inherence (something the patient is – biometrics).

The above distinction is more of a business use case distinction. From a technical perspective, a platform that has these two options configured can be created, with automation of the first use case (test-based user accounts) and manual creation of the second (or partial automation, if the situations to which it is applicable can be easily identified).

In either case, access to the content of this designated patient space should be limited to the patient. In this respect, best practice is for the individuals in contact center and reception not to have access to the authentication credentials of the patient or to the content of the designated patient space.

Further, access of patient family members to this designated space (in either cases) should be done only after careful analysis of legal requirements on confidentiality and exemptions in this respect. The option of family members should be embedded in the initial architecture of the designated space application, with proper segregation of duties in place (e.g. proposal of account access granting by one person and approval by another person).

The proposed solution ensure a higher degree of security and privacy (especially in terms of individuals having access to data) than giving medical test results via email (to the email provided by the patient) or to the email given by the patient in the contact center of the

healthcare organization. Having in place such types of communication methods increases the risk of data being sent to other individuals than the patients.

Nevertheless, if further contact is needed with the patient - .e.g. notifications about upcoming checkups, repeating tests, such information can be sent to the contact details provided by the patient (e.g. email, telephone number), with minimal health data being included in this communication, to limit risks of interception or wrong recipient due to inaccuracy of contact details.

Irrespective of the legacy systems in place within the healthcare organization, the adapting of existing IT systems and development of new IT systems as per the above requirements represents improved quality of patient care and security of data held by the healthcare organization.

The below figure shows the main principles to be had in mind when designing and developing the designed patient space.

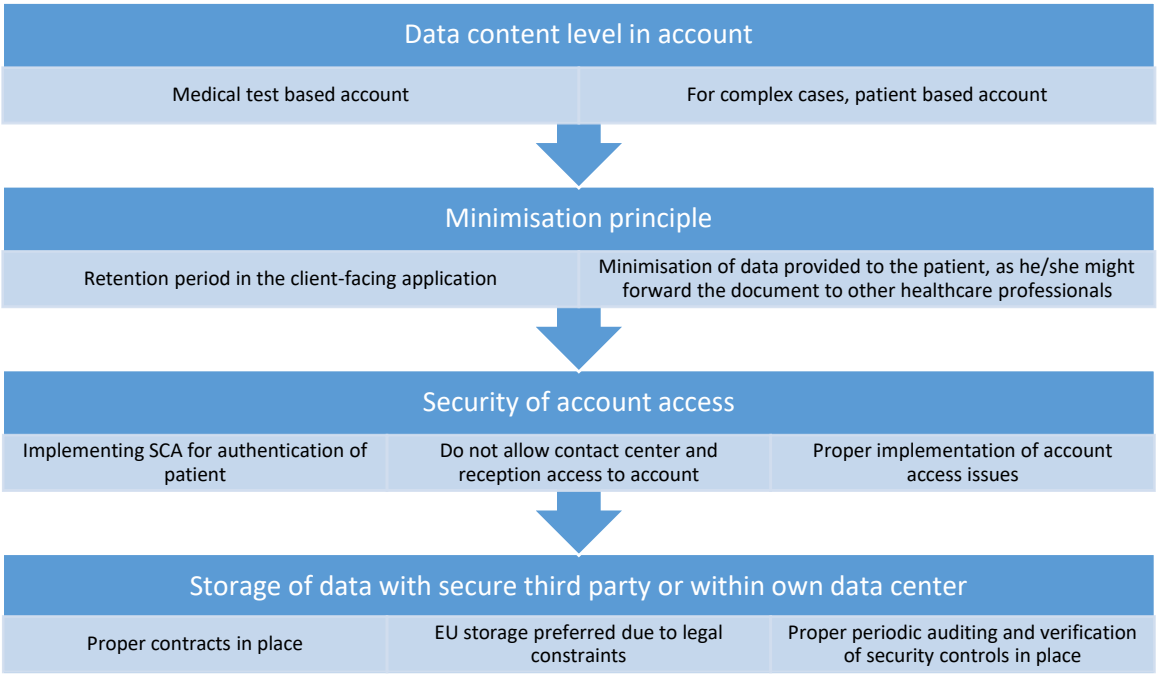

Figure 2 – Main principles for Patient-access data platform

4. Communication with other healthcare organizations

The specific solutions proposed in the previous section with respect to communicating data to patients can be applied to communication to other healthcare organizations.

Given the need to observe the confidentiality obligation concerning patient data, there are limited situations in which data can be shared directly with other healthcare organizations. Aside from urgent situations when the vital interest of the patient is at stake, in other situations, the consent of the patient for this transfer is needed.

Therefore, the use of an online platform is essential, with proper access management in place. This can be based on the specific patients, with an account being created per third party healthcare organization and for each patient separately. Alternatively, the access can be granted for the specific third party healthcare organization and for a specific medical test result.

Regardless of the manner in which the granularity of data is established, before granting third party healthcare organizations access to data, proper identification and authentication mechanisms have to be in place to ensure that the individual receiving the authentication credentials is in fact the representative of the third party healthcare provider. This can be performed by face-to-face means or, remotely, by specific authentication questions and double checks through various means – e.g. telephone, emails, official registries.

For transfer from third party healthcare organizations, the same principles can be applied. If the third party entity cannot provide a proper and secure manner of transfer, this can be created by the receiving healthcare organization.

When receiving health data concerning patients, confirmation from the sending entity about the consent (or fulfilment of other legal requirements) should be obtained prior to receiving the data together with confirmation that only the data needed by the receiving entity is being sent.

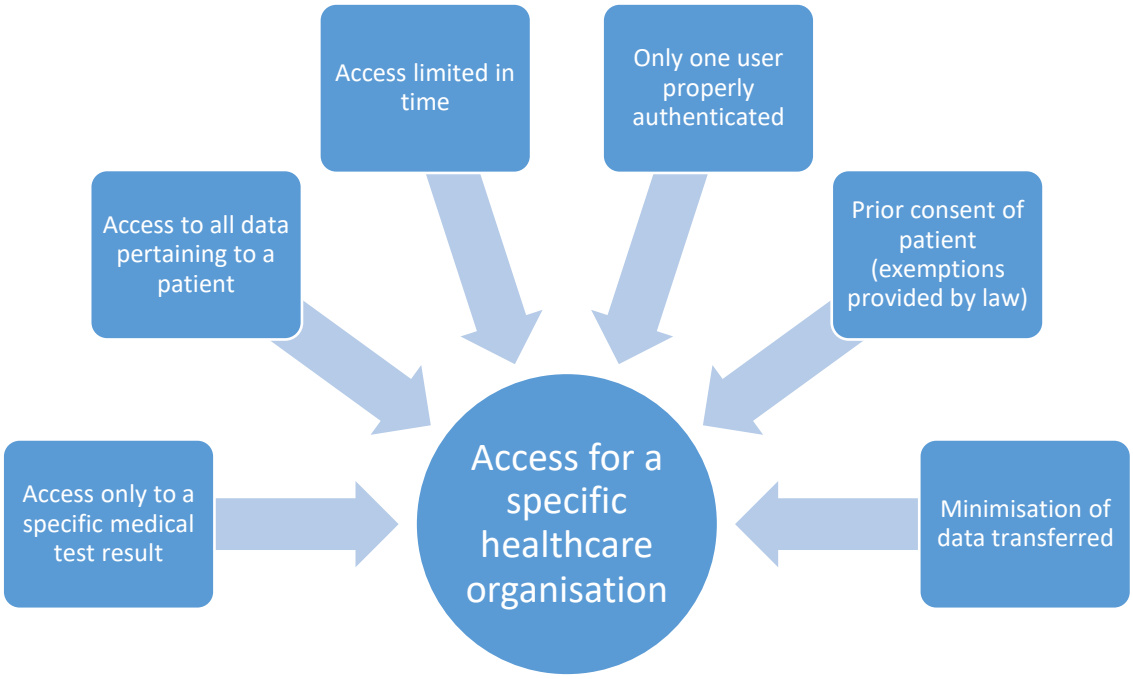

Figure 3 – Requirements for granting access to third party healthcare organization

In case of continuous transfer of data between healthcare organizations, APIs or dedicated user accounts for the other healthcare organization can be set in place or, at least a SFTP (e.g. for large files that need to be transferred) in order to transfer data securely. This should be accompanied by internal policies and procedures on the situations in which data can be transferred, which data can be transferred and the time limitation for the transfer.

5. Healthcare professional accessing data from outside the organization's network

There has been a wider use of BYOD in the past decade and this tendency has reflected also in the medical field. Even if email and share drives may be among the preferred options for viewing patient data, remote access to specific healthcare applications used by the healthcare organization is also being considered.

The practical recommendations outlined in this section have in mind a relevant NIST publication on BYOD and the specifics of the healthcare sector.[1]

[1] NIST, SP 1800-22 (Draft), Mobile Device Security: Bring Your Own Device (BYOD).

The first step relates to using only devices that are approved from a policy perspective, as they fulfil all the requirements in terms of security.

The second step refers to having the relevant Enterprise Mobility Management (EMM) software installed on the devices. This can be performed after

Using an EMM can help in a correlated and integrated approach towards BYOD and remote connection to resources of the healthcare organization. In this manner, proper BYOD policy can be implemented, with EMM in place and lack of possibility for the users to download the documents outside of the professional area.

Proper encryption or remote-wipe solutions for these devices can be contemplated as well, as they add layers of protection for the confidentiality of data. The remote-wipe solution is generally included in EMM solutions.

Further, EMM solutions generally have a policy checking in place that can analyze the mobile device and flag certain vulnerabilities. The policy can be configured such that the EMM solution does not permit access to the IT systems of the healthcare organization if the conditions in the policy are not met –e.g. non-rooted devices, no mobile apps potentially ranked as potentially having malware are installed, display protection is on.

6. General network structuring and access management principles

General principles about network structuring and user management should be had in mind, including the following main directions:

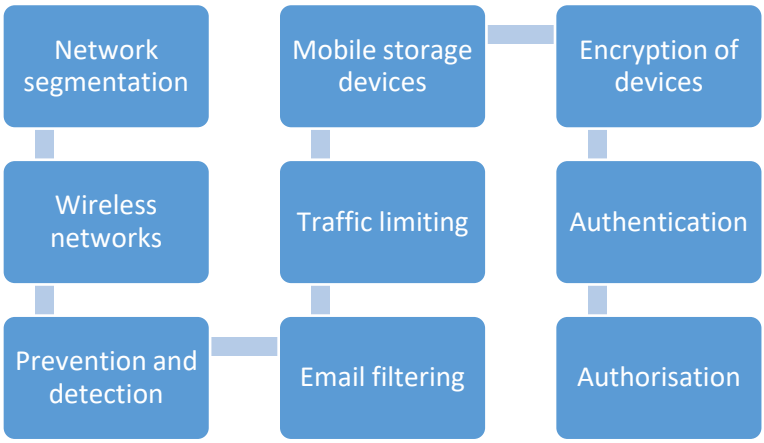

Figure 4 – General entry-level security principles for networking structuring and access management

- **Network segmentation:** Network segmentation is essential in keeping successful attacks from affecting multiple areas within the healthcare organization. The sections can be created based on the business areas within the healthcare organization and on the various data classification labels. For example, the medical devices will be kept in a separate network than the computers used by staff for communicating with the patient application server. Further, in case of clinical studies being conducted in the healthcare organization, the IT systems and data used for these should be held in a separate network.
  In addition, VPN should be used for remote access to data/IT systems of the healthcare organization.
- **Wireless networks:** Wireless networks are frequently used as entry-points for attackers and their design should be correlated to the network segmentation part. In addition, specific designated and separate wireless networks should be created for internally used devices (e.g. medical devices, computers), for the staff (with a hidden SSID) and for visitors (a general guest network).
- **Prevention and detection:** Prevention and detection mechanisms should be set in place at specific locations within the network structure (e.g. specific nodes, close to firewalls or at the host level in certain cases). Whereas IDS is aimed at detection of potential attacks, IPS can be used for prevention as well. In this case, there are many off-the-shelf customizable options. Further, a monitoring tool aimed at analyzing at least the network traffic and server communication can be considered.
- **Email filtering:** Emails are classic entry points for social engineering attacks and, on the long run, proper email filtering may be worth investing in.
- **Traffic limiting:** In view of helping further on the phishing side, aside from awareness training, one may contemplate limiting traffic towards certain types of websites from being accessed through work devices (e.g. computers, tablets). These may use a significant amount of bandwidth (e.g. social media, video streaming) and may also be entry points for social engineering attacks.
- **Mobile storage devices:** Even if this is more on the host side, a relevant aspect from a security perspective is the prohibition of using USBs on the organization devices. This ensures that the staff uses the designated channels for sending documents and limits exposure of data through mobile storage.
- **Encryption of devices:** The organization devices used within the healthcare activity should include proper encryption so that, in case they are lost, the data they contain cannot be (easily) retrieved by third parties.
- **Authentication:** For authentication in IT systems holding patient data, multi-factor authentication should be used in order to prevent access by attackers in case the passwords or account are compromised. Generally, this can be doubled by allowing

authentication with a user account only on one device at a time. In case the staff has to access multiple IT systems at a time, SSO may be contemplated for the remaining IT systems, after the first authentication takes place.

- **Authorization:** The staff should have proper access to data based on their job description. This can be set when a new employee (or an independent co-operator) starts work in the healthcare organization and the process for granting authorization can be correlated with the HR onboarding process. This assumes that, within the healthcare organization there is a central (or distributed) evidence of all employees and independently contracted staff for all departments.
  It is essential to keep the authorization level updated throughout the employment lifecycle. Any change in position or department has to result in a verification of the authorization needed for the new position. The rights of any leavers should immediately be deleted. Any temporary staff should have temporary authorizations set. Thus, for this employment lifecycle, the authorization updating can be correlated with the HR process in order to ensure accuracy of the data access/change rights granted to the employee.
  This authorization level is to be checked by each IT system/storage server accessed by staff members.

7. Availability of data and availability of IT systems - working towards resilience

An essential part of the protection of health data is its availability, as this may prove critical in most situations of interaction with patients. Further, the availability of IT systems is equally essential.

In order to achieve this, the first step is the identification of the time interval after which back-ups to be created at a different and separate location than the original servers.

The main purpose of such back-ups is for easy restoration into production if the original IT systems are compromised or fail. Thus, back-ups can be created online at a different location or offline (in case of data that can be easily restored – e.g. xml files, small databases). In case cloud solutions are used for storage of IT systems, the back-up can be integrated into the cloud service solution purchased.

Regardless of the back-up option chose, regular testing should be made to ensure that the back-ups can be restored to production easily and swiftly.

8. Conclusions

Whereas there are many areas to have in mind in order to ensure security, privacy and business continuity within a healthcare organization, this article aims at providing a starting point for the first steps in this respect, with minimal resources and costs.

The main focus in a healthcare organization is on availability of data, ease of secure communication within the organization and outside the organization (to patients or to other entities). In addition, given the mobility of staff members within the building of the healthcare organization and outside it, remote access to patient data has become more and more useful. The article includes basic bring your own device principles that can be easily implemented and scaled within the healthcare organization.

There are various manners in which the data (e.g. test results, medical records) can be transferred to patients or to other medical organizations. This article proposes specific solutions in this respect, outlining the practical implications and advantages thereof from a security, availability and privacy perspective.

We further outline, for either solution chosen, main networking, user management and business continuity principles to be had in mind, with practical examples of implementation, tailored to a healthcare organization and having in mind the usage of little resources for implementation.

It is also important that the above principles are replicated by all the entities involved in the supply chain of the healthcare organization in order to ensure, on the one hand, compliance with