IoT Security Reference Architecture for the Healthcare Industry

Release 1

Notices, Disclaimer, Terms of Use, Copyright and Trade Marks and Licensing

Notices

Documents published by the IoT Security Foundation (“IoTSF”) are subject to regular review and may be updated or subject to change at any time. The current status of IoTSF publications, including this document, can be seen on the public website at: https://iotsecurityfoundation.org.

Terms of Use

The role of IoTSF in providing this document is to promote contemporary best practices in IoT security for the benefit of society. In providing this document, IoTSF does not certify, endorse or affirm any third parties based upon using content provided by those third parties and does not verify any declarations made by users.

In making this document available, no provision of service is constituted or rendered by IoTSF to any recipient or user of this document or to any third party.

Disclaimer

IoT security (like any aspect of information security) is not absolute and can never be guaranteed. New vulnerabilities are constantly being discovered, which means there is a need to monitor, maintain and review both policy and practice as they relate to specific use cases and operating environments on a regular basis.

IoTSF is a non-profit organisation, which publishes IoT security best practice guidance materials. Materials published by IoTSF include contributions from security practitioners, researchers, industrially experienced staff and other relevant sources from IoTSF's membership and partners. IoTSF has a multi-stage process designed to develop contemporary best practice with a quality assurance peer review prior to publication. While IoTSF provides information in good faith and makes every effort to supply correct, current and high quality guidance, IoTSF provides all materials (including this document) solely on an ‘as is’ basis without any express or implied warranties, undertakings or guarantees.

The contents of this document are provided for general information only and do not purport to be comprehensive. No representation, warranty, assurance or undertaking (whether express or implied) is or will be made, and no responsibility or liability to a recipient or user of this document or to any third party is or will be accepted by IoTSF or any of its members (or any of their respective officers, employees or agents), in connection with this document or any use of it, including in relation to the adequacy, accuracy, completeness or timeliness of this document or its contents. Any such responsibility or liability is expressly disclaimed.

Nothing in this document excludes any liability for: (i) death or personal injury caused by negligence; or (ii) fraud or fraudulent misrepresentation.

By accepting or using this document, the recipient or user agrees to be bound by this disclaimer. This disclaimer is governed by English law.

Copyright, Trade Marks and Licensing

Acknowledgements

We wish to acknowledge significant contributions from IoTSF members to this version of the document:

John Moor, IoT Security Foundation
Richard Marshall, Xitex Ltd
Stacie Hoffmann, Oxford Information Labs Ltd

Peer Reviewers:
Darron Antill, Device Authority Ltd
Rosa Lenders, Device Authority Ltd
Claire B Milne
Plus others – you know who you are!

Contents

Executive Summary

The IoT Security Foundation is publishing this *IoT Security Reference For The Healthcare Industry* as part of a series of architecture documents. The aim of this document is to:

- Reduce/manage complexity of health-related IoT systems by highlighting trust and security management points to support a layered approach to security
- Demonstrate by example what a good health sector security regime looks like
- Demonstrate how to support security in IoT for health with minimal reliance on healthcare professionals and patients
- Explain the benefits of such an approach in a healthcare environment including achieving security goals, maintaining system hygiene and resilience, managing extensions and life-cycle provisioning
- Help foster growth and demand in the healthcare IoT marketplace and promote a security mindset for better-informed procurement decisions

Internet of Things (IoT) products and services have created a significant healthcare opportunity. They offer benefits such as improved diagnosis and treatment, the ability to carry out remote monitoring, and reducing operating costs to counter the rising cost of care. Additionally, IoT products that were not specifically designed for healthcare use are being used in this sector. The majority of existing healthcare products were designed to operate in a controlled environment, like hospitals or healthcare centres, where there can be controls for both physical access and device connectivity. However, the inherent connectivity of IoT devices and potential for remote or mobile features undermines existing security controls by the very nature of the deployment.

This paper addresses the mounting risks associated with the increasing use of IoT products in a health-related ecosystem, including confidentiality and integrity of devices and data, and availability of communications. It takes into account factors such as the importance of data integrity for systems as well as physical health and safety, decreased control over devices functioning outside a local network, and increased flow of data in and out of local networks. Building on this, the document provides example architectures that take into consideration practical technical and network elements to support successful and secure deployment of health-related IoT. This is first explored through four use cases: fixed devices (e.g. MRI scanner), portable local devices (e.g. vital signs monitor), portable loaned devices (e.g. blood pressure monitor), and personal devices (e.g. hearing aid).

From the four use cases, three different network environments are mapped and architectures explored: “bounded”, “boundaryless” and “hybrid” environments. Central to these architectures is understanding different security needs and data flows within and outside the local health environment, points of interconnection between networks (including segmented intranets and connection with the public Internet) and devices, and threat vectors. In particular, the architectures focus on incorporating security and design best practices to support layered security of devices and networks and patient data protection and privacy.

A layered approach to security is useful in environments such as the health industry due to the ability to provide additional protection for legacy and new IoT products with varied security capabilities, and support data and network security (e.g. protection from mobile devices migrating between public Internet and local networks). This document aims to inform those adopting and deploying IoT for health solutions, as well as to inform and influence those developing IoT products, the *Intended Audience* is provided in Section 1.2.

For the purposes of this document, an IoT for health device can encompass a variety of IoT products found on the consumer (e.g. hearing aid) and medical industry (e.g. MRI scanner) markets. The key feature that links these products and markets is the automated collection of an individual’s health-related data, and their ability to share that data over communications networks (either remotely or locally) with healthcare professionals (such as clinics, laboratories, and physicians). The interchangeable terms “health-related IoT device” and “IoT for health device” used in this document largely reflect the common understanding of the term “digital health device”. A few subtle differences pertinent to this document are explained in the Section 1.3, *Scope*.

1 Introduction

A growing number of health-related IoT devices are currently available in the marketplace, each incorporating different aspects of the reference architectures explored in this document. Before standard solutions are available, health device developers, OEMs and IT managers should be able to identify the primary IoT and security management needs for their IoT for health solutions by using this reference architecture in conjunction with suitable risk assessment, such as international standard ISO/IEC 27001:2013 [ref 52] and ISO process for risk management of networked medical devices [ref 20]. With this information, developers, OEMs and IT managers may then identify those available good security practices and market solutions that are best suited for their own IoT deployment. In particular, readers should consider:

- Security needs for each unique adoption of IoT in the health industry
- Threats associated with adoption of new services and technologies outside bounded networks, such as cloud services, outpatient care, and the use of data from personal or mobile devices in healthcare
- How to support more comprehensive security solutions in health-related IoT devices from the outset of design

Section 2 introduces the approach to security principles used in this document. Four use cases are then explored in Section 3, Architecture Use Cases and Assumptions, to:

- Consider the risks associated with IoT for health devices and services
- Identify possible trust or security management points in the different architectures

Section 4, Reference Architectures*,* expands on the uses cases to provide environment mapping and security concerns in three network architectures.

Finally, in Section 5, High Level Requirements are listed to support adoption of the recommended architectures to mitigate risks identified during the preliminary threat modelling and assurance studies.

1.1 Intended Audience

Patients and end users are not the intended or expected target audience for this document. The intended audiences and relevant sections to people with those roles or responsibilities are:

- IT departments and purchasers working in health-related environments (e.g. hospitals, general practitioner or physical therapist offices) – to better inform security-focused IoT management and architecture, and support better-informed purchasing decisions, particularly:
    - Section 2: Security Principles
    - Section 3: Architecture Use Cases and Assumptions
    - Section 4: Reference Architectures
    - Section 5: High Level Requirements
- Healthcare systems/service providers – to better understand the security needs and requirements of health-related IoT environments and how the provider's systems/services interact with that environment in order to provide appropriate systems or services that support security best practices:
    - Section 2: Security Principles
    - Section 3: Architecture Use Cases and Assumptions
    - Section 4: Reference Architectures
- Developers of IoT for health devices – to better understand IoT management and security needs of health-related IoT environments and solution development opportunities in the market, particularly:
    - Section 4: Reference Architectures
    - Section 5: High Level Requirements
- OEM Product Management – to better understand IoT management and security needs of health-related IoT devices and environments so that they may produce solutions which fill gaps in the market, particularly:

- Section 4: Reference Architectures
- Section 5: High Level Requirements

1.2 Scope

This document presents technical and network architectures specifically for the health sector with to broaden the understanding of associated risks and high-level thinking about protecting internal health systems and patient data from external risks. Personal devices sharing data with healthcare professionals may be conceptualised as one such risk. By examining architectures for a range of devices (such as those in **Figure 2***)* and their security implications, we aim to promote best practices for health-related IoT solutions and to ensure that specifiers, designers and implementers can identify security measures that are appropriate for their particular deployment.

We have based our interpretation of "health" on the World Health Organisation constitution [ref 53], which includes all aspects in **Figure 1**:

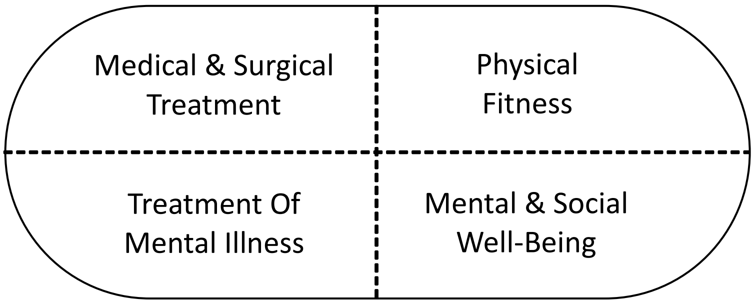

Medical & Surgical Treatment
Physical Fitness
Treatment Of Mental Illness
Mental & Social Well-Being

Figure 1: Health Aspects

The Internet of Things for health sits within the broader field of digital health. Digital health is the merging of digital technologies with health and care. The US FDA includes mobile health (mHealth), health information technology (IT), wearable devices, telehealth, telemedicine, and personal medicine in this broad category [ref 53]. For instance, mHealth may include health services 'supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices' [ref 54]. **Figure 2** demonstrates areas of overlap between IoT for health and digital health.

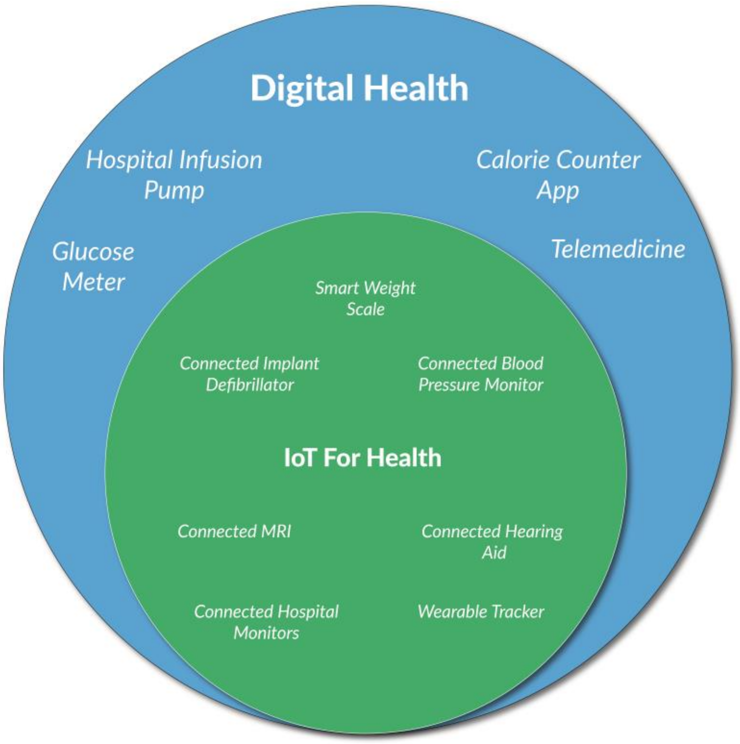


Figure 2: The IoT for Health Landscape

The scope of digital health is therefore related to but wider than the IoT for health considered in this document. The differentiating factor is the automated collection, and sometimes external sharing, of personal data for use by health professionals providing care to that individual. Digital health subcategories (such as mHealth or telemedicine) which do not fit this criteria are not considered here. For comparison, the IoT devices that support delivery of subcategories such as mHealth may be considered within scope. Health IT – use of information systems in healthcare – is closely related as this document proposes an architecture to support security, but the broader area of health IT is not the primary focus of this document.

Devices owned/operated by the health service provider and personal devices which may share information about the patient with the health provider (such as hearing aids) are the focus of this document. However, the specifications related to the design and manufacturing of personal consumer devices (e.g. connectivity, functionalities, security capabilities) are out of scope for this document.

Mobility	Health Provider Owned & Managed	Patient Owned & Managed
Fixed	MRI Scanner	N/A
Portable	Vital Signs Monitor Blood Pressure Monitor	Connected Hearing Aids

Table 1: Key IoT Device Characteristics

Security factors in the deployment of health-related IoT devices are varied; this includes factors such as the network architecture in which IoT devices exist, the technology that provides device connectivity, device portability, and device ownership/management. The factors of mobility and ownership laid out for reference in

Table 1, above, are used to identify the use cases and how they apply to architectures described in this document

A poorly secured device may have serious negative impact on the patient or the ability to deliver effective care. Additionally, different types of devices require different security considerations – for example security specifications will be different for connected hearing aids and a connected MRI scanner. As a result, subsequent sections of this document (Section 4, Reference Architectures, and Section 5, High Level Requirements) take both the environmental features and the IoT devices into consideration.

Accidental malfunction of hardware or software is out of scope for this document, but we note that reliability engineering is a discipline of its own, fault tolerance is designed into some medical equipment, and reliability and safety are not always aligned [ref 17]. Additionally, this document does not focus on threats from actors with enough resources to circumvent good security practices in standard versions of an IoT health product[1].

Instead, this document concentrates on countering common threats for regular use cases, as opposed to highly targeted or selective attacks. The focus here is on finding the right balance between factors such as security, technical capability, economics and the risk appetites of healthcare providers. The aim is to provide architectures for general use cases that support this balance.

1.2.1 Reported Vulnerabilities in Health Devices

Research shows a growing list of publicly reported security vulnerabilities in IoT devices and services. Recorded vulnerabilities related to IoT for health go back to 2008, and vulnerabilities are being found at an increasing rate – likely due to the increasing number and variety of devices in use, and vulnerability research. Some examples of medical devices and their discovered vulnerabilities are provided in Table 2. It should be noted that this list is for illustration and is not exhaustive; the impacts on security for each vulnerability are more wide reaching than presented here.

Date Disclosed	Device Type (Manufacturer)	Vulnerability	Potential Impact On Security
19 May 2008	Implantable Defibrillator (Medtronic)	Remote access	Direct impact on the safety of the device for the user • Hackers remotely accessed a heart defibrillator and pacemaker • Hackers shut down the device • Hackers made device deliver electric jolts
13 June 2013	Medical Devices (multiple)	Hard-Coded Passwords	Increased vulnerability to attacks such as command and control or malware • Inability of users/owners to change passwords manually • Potential for "mass hack" of devices with same or similar passwords • Use of connected environments for downstream attacks
10 June 2015	Patient-Controlled Infusion System (Hospira LifeCare)	Connected Devices and Systems	Direct impact on downstream security and safety of the device for the user • Vulnerability allowed hackers to remotely command and control • Exploitation could impact delivery of medication via the bloodstream
08 July 2018	Fitness Tracker Data API (Polar)	Personal Data Collection	Direct impact on user privacy and data protection as a result of non-medical uses • Access user location data • Identify names and addresses of users • Identify military personnel and locations

Table 2: Vulnerabilities and Potential Impacts

[1] For example, the different security concerns for a high-profile individual's pacemaker as compared to the average user.

Some of these vulnerabilities had the potential to cause considerable physical harm, including death, to users if exploited. Fortunately, these vulnerabilities have yet to be exploited in these ways. Nevertheless, we recognise the need for rapid and significant improvement in the security of health devices, as untreated vulnerabilities will be more damaging and commonplace in the future.

1.2.2 Looking Ahead

The IoT for health market is evolving and effecting change in the threat landscape for health service providers. Risks associated with IoT for health are, generally, not considered by existing medical device regulations which have not kept up with the market. Currently, IoT for health-specific solutions, business models, or regulations setting guidance and best practice are nascent. These reasons, among others, are why this architecture aims at bridging that gap by providing a reference point for service providers, developers and manufacturers in the healthcare industry.

Complexities associated with the IoT for health environment that need to be taken into account as devices and services develop include:

- Confidentiality, integrity, and availability of data including patient information;
- Authentication of users and devices;
- A variety of device ownership models (e.g. owned by an individual or by a healthcare provider);
- Environments (e.g. a single doctor’s office, a national healthcare system, or home);
- Network technologies (e.g. Wi-Fi and Bluetooth); and
- Stakeholders (e.g. patients, service providers and healthcare professionals)

There will not be a single solution for the issues that arise in IoT for health and best practices will take time to emerge. This is partially due to the role that jurisdiction will play through regulations, markets, and industry structure. Societal expectations of healthcare, confidentiality and data flows/management will also influence solutions as will various actors’ interests in specific aspects of the service chain – such as device ownership and management, data storage, etc.

For example, local industry structures (e.g. healthcare as a public service or as a private industry) will influence investment and procurement models as well as ownership expectations of particular IoT-related deployments. With this in mind, will devices be wholly owned by the healthcare provider or provided as a managed service by a third-party? Will data be held in a third-party service provider’s cloud server or in the health service provider’s private servers?

Developing this architecture also brought to light a number of questions regarding consumer IoT and the health industry. For example, how can health providers verify and trust data from a patient’s device? Additionally, how can this data be efficiently and securely integrated with the health provider’s systems?

It is conceivable that in the future there will be health sector certified or compatible consumer devices that are designed to address these questions. For instance, a patient’s mobile phone may use an app to authenticate to their personal health service database and directly share information. Inversely, a doctor may be able to send a data request to the patient’s device and the patient will be able to consent to that data share at the push of a button.

Although there are no sector-specific regulations that address security concerns, there may be other IoT-related regulations or standards that can be adopted while sector-specific solutions are developed. Health-related consumer and medical grade IoT devices overlap with general regulations such as competition, consumer protection and data protection regulations as well as other policies directly related to digital technologies (see IoTSF’s white paper *IoT Cybersecurity: Regulation Ready* for more information [ref 56]). Overlap is likely in areas where the performance of a compromised medical device can negatively affect and individual’s physical safety or wellbeing, their privacy, enable misuse of personal data, or result in negative repercussions for downstream stakeholders (e.g. health providers or patients).

This architecture is attempting to address many difficulties posed by IoT for health, without knowing how the market will evolve, the type of services to be provided, or ownership/management structures of data and devices. This begs the more fundamental question: does IoT for health require a unique approach to security? There is still much work to be done in this area, and this architecture presents few problem areas and what potential solutions might look like. Possibly the most difficult aspect of solutions development will be achieving a good level of security without putting onus on the patient or healthcare professional.

1.3 Taxonomy & Definitions

1.3.1 Taxonomy

In the requirements sections, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119 [ref 50].

1.3.2 Definitions

Health — A state of complete physical, mental and social well-being and not merely the absence of disease or infirmity [ref 53].

IoT for Health — IoT devices or products that collect, and sometimes share, personal data in an automated manner for use by health professionals providing care to that individual.

2 Security Principles

There is a wide variety of devices that could be considered "IoT for health" and equal variety in the level of security features they support. Those deploying IoT for health devices and products need to be aware of the broad range of security risks - from network security to data protection. Implementers should take common security principles and IoT security best practices into consideration from the outset. IoT for health will not be the same in every case, so resulting decisions will differ by deployment.

A modest approach to security focuses on the following three key principles, also included in the "IoT Security Compliance Framework" [ref 44] [2]:

- Confidentiality – ensuring information and systems are protected from unauthorised access
- Integrity – ensuring that information and systems are unaltered and accurate throughout the lifecycle. For instance, information integrity applies to data collection, transfer, use and storage
- Availability – ensuring that information is and services are accessible by users or systems as and when needed

From these principles, a wide variety of questions emerge when considering IoT solutions. Many of these questions are considered in "Make it safe to connect: Establishing principles for Internet of Things Security" [ref 45] by the IoT Security Foundation, replicated here for ease:

- Does the data need to be private?
- Does the data need to be audited?
- Does the data need to be trusted?
- Is the safe / timely arrival of data important?
- Is it necessary to restrict access to, or control of, the device?
- Will the device need to be updated?
- Will ownership of the device need to be managed or transferred?

Developing these points to take into consideration architectures as well as data security, the proposed architectures expand upon the list above to support IoT for the health environment. Some architecture-specific questions are:

- Does the health provider need to segment local networks?
- To what extent does the health provider need to take into consideration legacy devices and varying degrees of device security capabilities?
- How can the health provider protect local networks and data from devices connecting remotely or wirelessly?
- How the devices are provisioned (e.g. configured, updated, access controls managed)?
- To what extent do health professionals and/or patients have access to the device?
- How can patients share data with health professionals securely and with consent?
- How and when is authorisation managed, shared and/or transferred between users?

Good security hygiene should be the foundation of any IoT management process. Therefore, the principles for this architecture are based on ensuring at least a minimum level of security across the health-related IoT ecosystem and understanding where weak points or attack vectors might be located. Below are a few examples of how the CIA triad intersects specifically with the health-related IoT environment.

[2] Some security practitioners, for example in cryptography, include other principles such as authenticity or non-repudiation, but this document focuses on the "information security triad" outlined above. Authenticity and non-repudiation are considered to be properties of the Integrity category for the purposes of this document [ref 18].

2.1 Confidentiality, Integrity and Availability

This section gives a few examples of the overlap between the traditional security principles of confidentiality, integrity and availability in a health-related environment. Confidentiality risks include risks to patient privacy and data protection through the collection and sharing of patient information between devices and systems (e.g. between personal hearing aids and a doctor's office). These risks are defined in many national and regional regulations, such as data protection regulations in Europe and health sector regulations in the US. As patient data is used for medical research, privacy considerations such as protecting the identity of individuals is also a key concern. Only those with authorisation and legitimate purpose should be able to access patient data and accessibility may vary by user – such as first responders versus nurses or general practitioners.

Integrity risks arise where changes in data might affect an individual's healthcare, either in terms of medical treatment, diagnosis, or more general health and fitness. Using IoT devices, both consumer and medical grade, to monitor health allows an increase in the amount and variety of information a doctor may take into consideration when treating a patient. More data and more data sources, however, heightens the risk of compromised or miss-analysed data. Compromised data integrity may result in impacts ranging from minor, such as miscounting a patient's steps, to serious, such as administering a harmful dosage. This is further exacerbated by the implementation of automated IoT products and services in health-related environments.

Availability risks can result from Internet-borne malware – such as ransomware or Denial of Service (DoS) attacks – that are not necessarily targeted at health services but affect the healthcare sector as a side-effect of a more general attack. Being unable to record monitor readings, access patient medical history or use resources such as connected thermometers can cause widespread disruption and harm to patients. A recent example of the disruption that can be caused by an attack is the impact of WannaCry ransomware on the UK's NHS in 2017 [ref 55].

3 Architecture Use Cases and Assumptions

This section briefly describes and provides background for the four categories of use cases in this document. For each use case, some of the motivating reasons to use connected devices are provided, background information pertaining to data flows is described and assumptions relevant to the use case are outlined[3].

3.1 Fixed Use Case: Connected MRI scanner

The fixed use case example centres on a connected MRI scanner, a type of connected diagnostic equipment, to demonstrate the risks and security considerations for connected health devices. There are several reasons for wanting to add network connectivity to devices like MRI scanners, such as image transfer and storage, remote control and management, consumable monitoring, and capacity planning. More information on these reasons is in Annex B1. Fixed Use Case: Connected MRI Scanner.

The fixed use case is particularly relevant to the bounded network architecture in Section 4.2. **Figure 3** demonstrates a patient's information flow when using a fixed IoT health-device such as a connected MRI scanner.

[3] For more background information on the use cases, why they were chosen, and how this impacted their categorisation, please see Annex B.

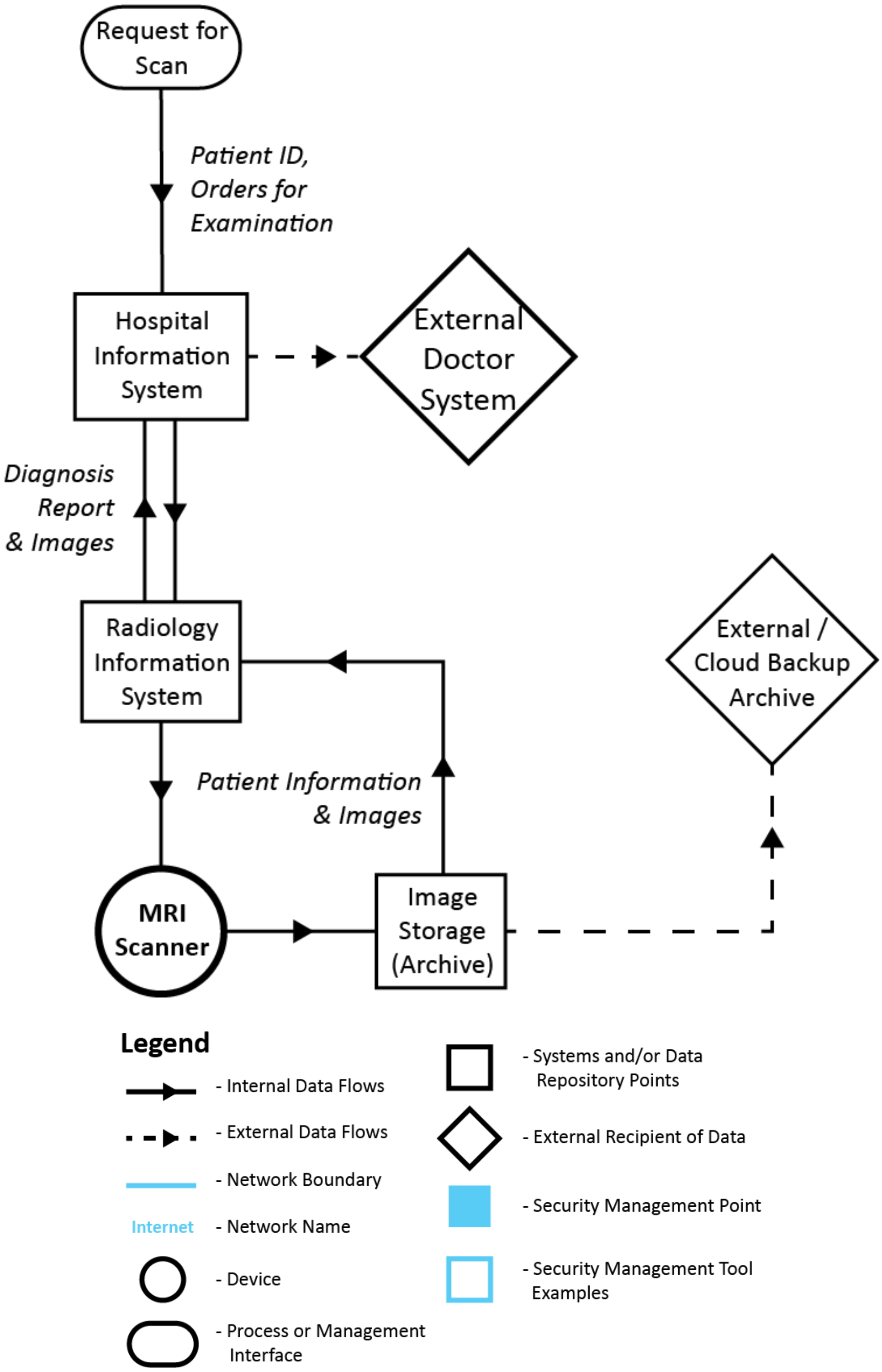

Request for Scan
Patient ID, Orders for Examination
Hospital Information System
External Doctor System
Diagnosis Report & Images
Radiology Information System
External / Cloud Backup Archive
Patient Information & Images
MRI Scanner
Image Storage (Archive)
Legend
- Internal Data Flows
- External Data Flows
- Network Boundary
Internet
- Network Name
- Device
- Process or Management Interface
- Systems and/or Data Repository Points
- External Recipient of Data
- Security Management Point
- Security Management Tool Examples

Figure 3: Patient Information Flow for Connected MRI

The different lines, boxes and colours used in **Figure 3** to **Figure 13** add information. For instance, arrows denote the directional flow of data, while the line type (e.g. solid or dotted) helps to identify whether data flows are internal or external. Although the solid and outlined blue boxes are listed as "security management" they could equally be "trust management" points or features.

In a fixed use case, data mainly flows within the health provider's local networks. However, different departments or network segmentations within the health provider's local network may require additional layers of security (e.g. radiology department systems vs the hospital's general information system). Additionally, data created and used within the health provider's network may be shared outside the network (e.g. sharing reports with external doctors or transfers to cloud service backup systems).

3.1.1 Assumptions: Fixed Use Case

For this use case the MRI scanner is considered a permanent fixed installation that is part of a larger healthcare facility, such as a general hospital. Such a facility is likely to have its own intranet, but physical protection of the local area network (LAN) might be poor as many visitors would have access to the building. Additionally, networks such as intranets should be configured in a way to protect devices with a variety of security capabilities, such as legacy devices, from incoming threats such as malware.

3.2 Portable Local Use Case: Hospital Vital Signs Monitor

This use case focuses on monitors that may be ported with the patient within the health service environment. The portability of the devices within a dedicated environment separate it from fixed equipment such as MRI scanners and loaned mobile devices, such as blood pressure monitors or personal devices used outside of a hospital or clinic.

Traditionally nurses use mechanical devices to perform patient observations (temperature, blood pressure and pulse) and manually record them on charts. This process has been identified as somewhat error prone [ref 27] leading to the introduction of automation, for both for observation and recording.

With modern technology, there are several reasons for wanting to use a portable vital signs monitor, such as automatic data upload, settings configuration, time synchronisation and firmware update. Please see Annex B2. Mobile Use Case: Wireless Connected Hearing Aids for more information.

The portable local use case may be relevant to all three architectures in Section 4. **Figure 4** shows a patient's information flow when using a portable IoT health-device such as hospital vital signs monitor.

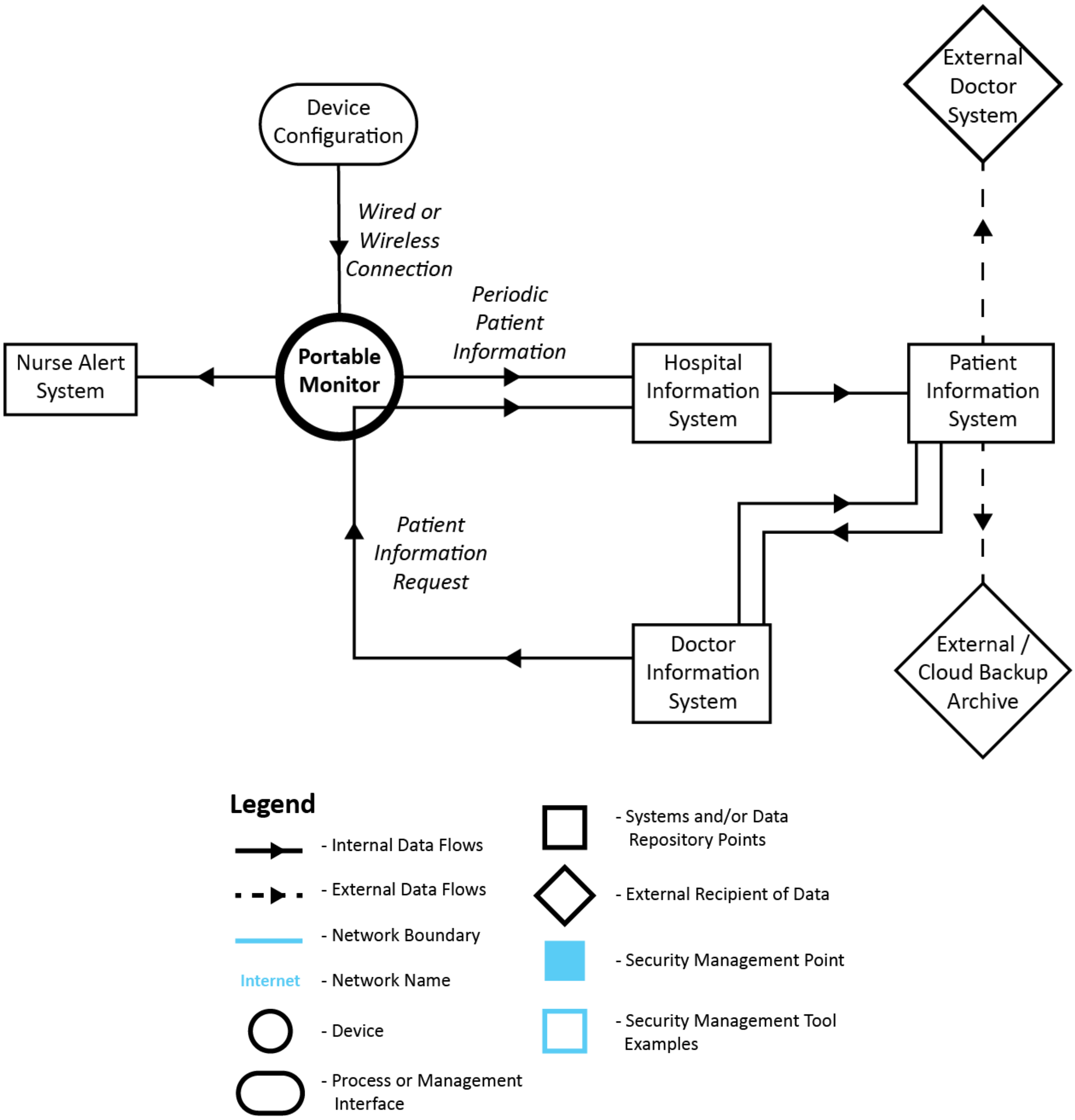

Device Configuration
Wired or Wireless Connection
External Doctor System
Periodic Patient Information
Nurse Alert System
Portable Monitor
Hospital Information System
Patient Information System
Patient Information Request
Doctor Information System
External / Cloud Backup Archive
Legend
- Internal Data Flows
- External Data Flows
- Network Boundary
Internet
- Network Name
- Device
- Process or Management Interface
- Systems and/or Data Repository Points
- External Recipient of Data
- Security Management Point
- Security Management Tool Examples

Figure 4: Patient Information Flow for Vital Signs Monitor

In this use case, while most data flows within the health provider's local area networks (LAN), information can be shared externally – such as with other doctors or backup archives – within a wider health system or outside that system.

A security gateway is particularly suited to be placed at different points of interconnection between networks and integrity zones (e.g. hospital information system and patient information system) to support appropriate security for devices, data, and networks. For instance, local networks such as intranets should be configured in a way to protect devices with lesser security capabilities, such as legacy devices, from incoming threats like malware.

To support good security practices, a security gateway may help segment a LAN into different zones with appropriate expectations of integrity. For example, multiple devices may be connected to a monitoring station which oversees categories of devices or receives alerts from those devices – such as for automatic remote alerting for rapid response, particularly if located in environments such as an intensive care unit (ICU). A security gateway could be implemented to act as or support the monitoring station. See **Figure 10** in section 4.3 for more information.

3.2.1 Assumptions: Portable Use Case

It is assumed that portable monitors will be owned by the healthcare provider and generally remain within the vicinity of the healthcare facility. No assumptions related to connectivity technologies are made. This is because devices may connect using a variety of network technologies, or via a local IP-based LAN. As such, no detailed assumptions are made about the environment in which the portable monitor functions other than the healthcare environment adopts network and information security best practices.

3.3 Portable Loaned Use Case: Blood Pressure Monitor

Loaned portable devices can be conceptualised as owned by the healthcare provider but used by the patient. Devices are not constrained to one dedicated environment and may be ported with the patient to a single remote location (e.g. nursing home, rehabilitation facility, or private residence) or be as mobile as the patient (e.g. ported to home, work, gym, shopping, used overnight, etc.). Given the nature of the device and its integration into the patient's daily life, the patient is likely to have more control over and engagement with this type of IoT device than in the fixed or portable use cases.

Reasons for adopting loaned mobile devices are similar to those for the portable use case. The appropriate healthcare professional(s) may have the ability to remotely provision the loaned device – this may include provision controls commensurate with a user's access control. Remote capabilities may include configuring the device (e.g. access controls) or adjusting functions (e.g. reading intervals or dosage release), requesting data from the device (e.g. blood pressure readings), and sending information to the device (e.g. software updates). In addition, loaned mobile devices allow the patient a wider range of independence (e.g. remote monitoring from home or work instead of in-hospital) and may improve patient healthcare as well as free up constrained health facility resources (e.g. bed spaces). Concurrently, the confidentiality and integrity of the data will need to be ensured. Please see Annex B3. Portable Use Cases: Hospital Vital Signs Monitor for more information.

The portable loaned use case is particularly relevant to the boundaryless and hybrid architectures in Sections 4.3 and 4.4. **Figure 5** is an example of a patient's information flow when using a loaned portable IoT health-device, such as portable blood pressure monitors:

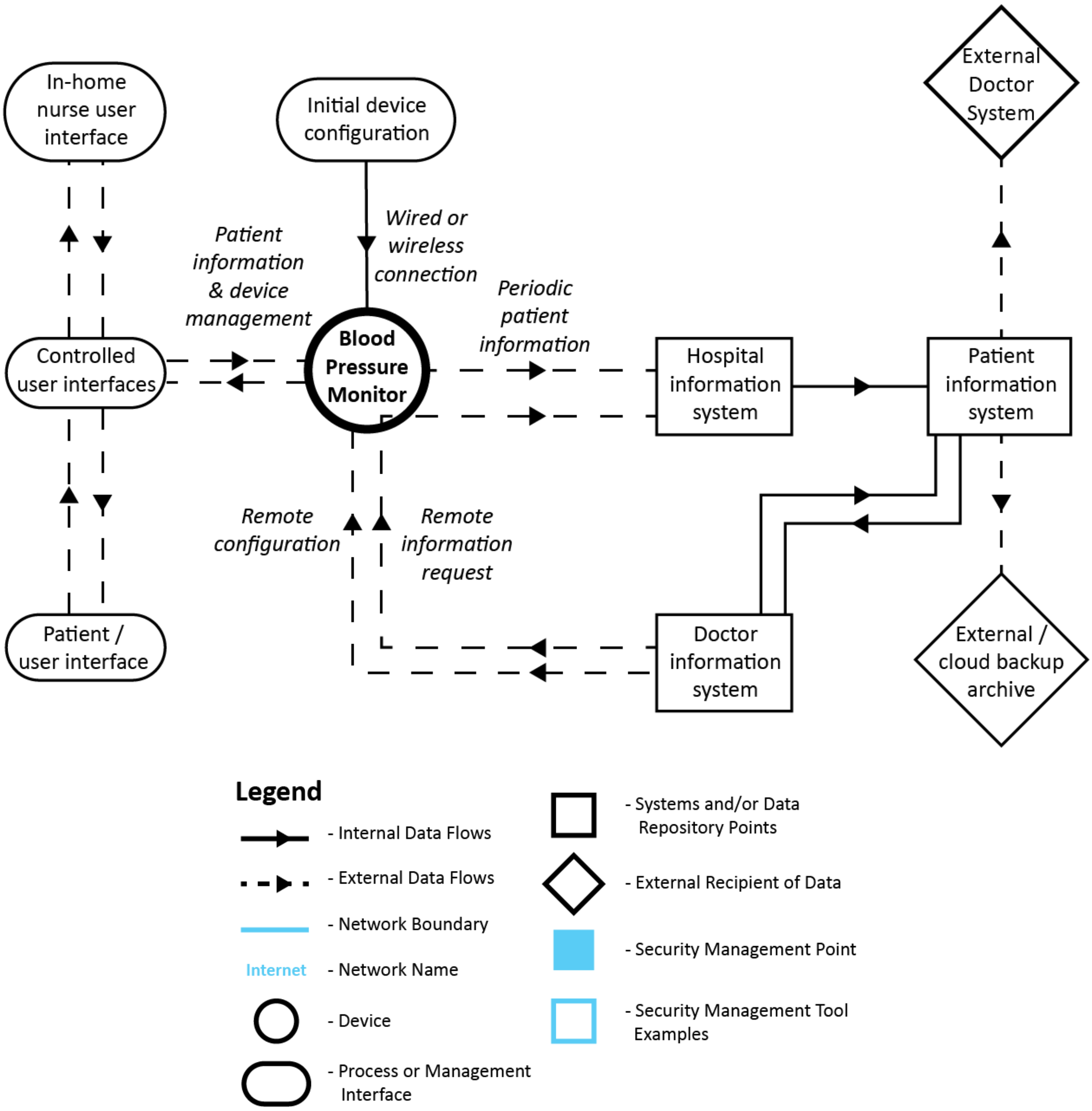

In-home nurse user interface
Initial device configuration
External Doctor System
Wired or wireless connection
Patient information & device management
Periodic patient information
Controlled user interfaces
Blood Pressure Monitor
Hospital information system
Patient information system
Remote configuration
Remote information request
Patient / user interface
Doctor information system
External / cloud backup archive
Legend
- Internal Data Flows
- External Data Flows
- Network Boundary
Internet
- Network Name
- Device
- Process or Management Interface
- Systems and/or Data Repository Points
- External Recipient of Data
- Security Management Point
- Security Management Tool Examples

Figure 5: Patient Information Flow for Blood Pressure Monitor

For a loaned device it is possible for a monitor to use mobile connectivity to share data with the healthcare provider. However, the device may also have an option to connect to Wi-Fi when mobile connectivity is not available. In this use case, data flows between the health provider's local networks and external networks. Security management features can be placed at the point of interconnection between incoming traffic and the LAN to protect the local network from external threats. For example, a firewall, authentication and authorisation, and traffic routing may be implemented.

3.3.1 Assumptions: Loaned Portable Use Case

No assumptions are made about the environment in which the loaned device functions – such as the use of a LAN or implementation of security features such as firewalls or gateways – due the high variety of and lack of control over the device's local environment at any given time. Unknowns such as this create a complicated environment for healthcare providers to implement and maintain good security practices. For this reason, it may be more appealing for healthcare providers to rely on a connectivity solution which they have a degree of control over – likely cellular technology in this use case. It is also assumed that device configuration will take place before/after each use or change of patient. However, these aspects will also depend on the capabilities of the device itself, and consideration of back-up connectivity solutions particularly for life-critical devices.

3.4 Personal Device Use Case: Wireless Connected Hearing Aid

Hearing aids are a common personal medical device[4], and there has been a continuing trend of miniaturisation to improve comfort and aesthetics. Modern in-canal hearing aids can be effectively invisible in normal use. Their very small size means that it is impractical to have volume controls on the hearing aid itself. As a connected digital device that is always worn, there is an inclination to converge functionality with other portable electronic devices[5], such as syncing with smartphones or music and games consoles. This is similar to convergence trends seen in the past, such as mobile phones replacing separate cameras and watches; the "hearables" convergence trend, however, may be limited by the small battery size and limited capacity.

The ability to request information from the patient via the medical or consumer grade personal devices (e.g. a connected pacemaker or consumer hearing aids) is a useful feature. Relevant information may include pre-set options and configuration, usage data, or noise levels. The process should ensure both patient consent and efficient information sharing. This may include instances where a patient is admitted to an emergency room and timely access to relevant data may be valuable information for the treating doctors to provide improved healthcare to the patient.

With modern technology, there are several reasons for wanting to use wireless connected hearing aids such as mobile device operating controls and monitoring, remote care, use as a mobile phone headset, audio playback and linkage to home automation.

The personal device use case is particularly relevant to the boundaryless and hybrid architectures Sections 4.3 and 4.4. **Figure 6** is an example of a patient's information flow when using a mobile IoT health-device, such as connected wireless hearing aids:

[4] A 2015 survey (MarkeTrak 9) estimated that they are used by 3.2% of the US population.

[5] This convergence even has a new buzzword: "hearables".

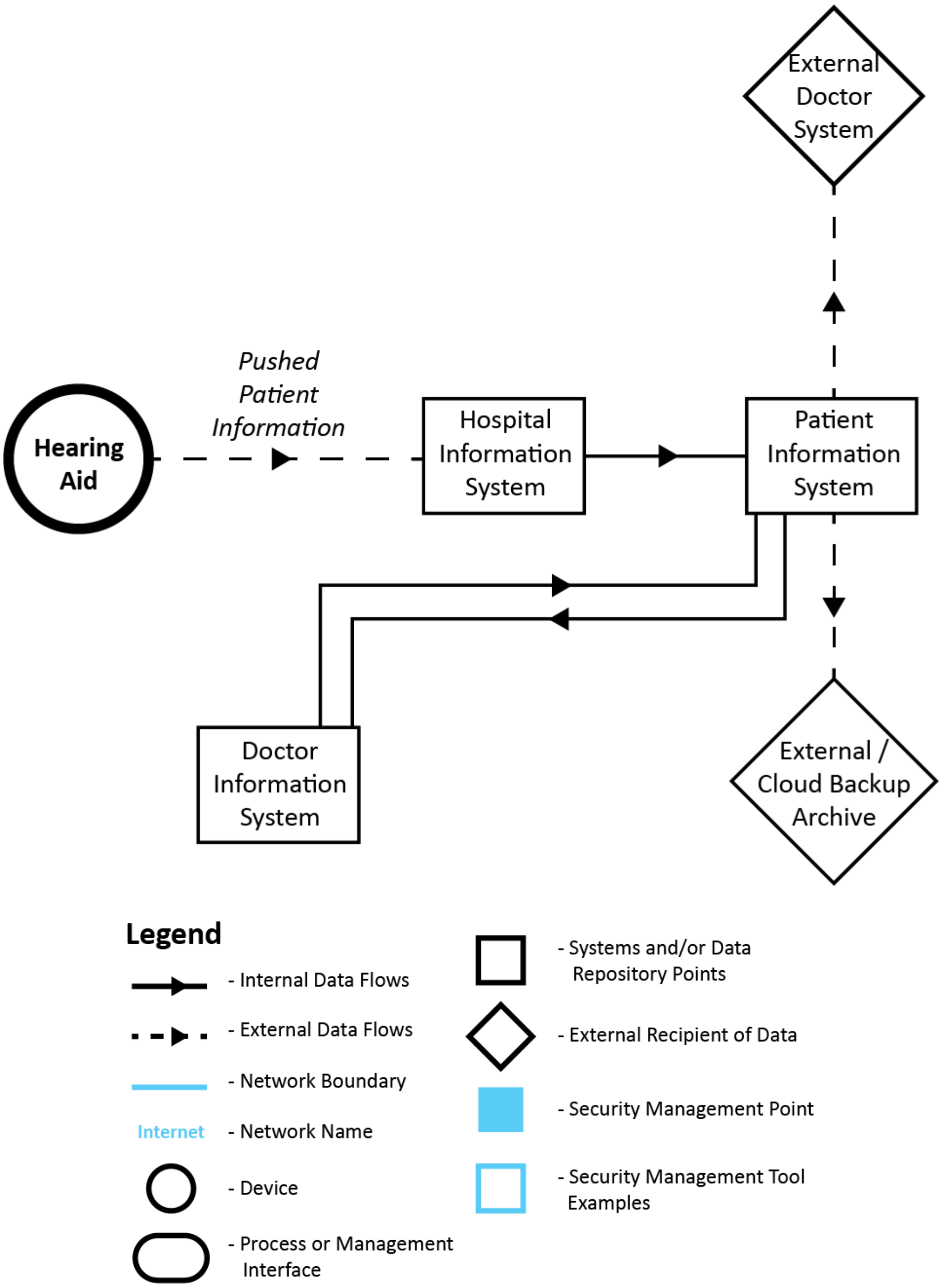


Figure 6: Patient Information flow for Personal Device

A plethora of consumer-grade health-related IoT devices are already on the market. This includes devices such as connected hearing aids and glasses, and wearable monitors that track health-related information, such as sleep, steps, weight, and heartrate. It is important for healthcare providers to understand the risks associated with requesting patients to share data from personal devices – such as malicious data entering the local healthcare system and difficulties associated with data verification and integrity impacting healthcare.

Implementing security controls at trust boundaries helps adopt a layered security approach to protect internal systems from external threats like incoming data from personal devices. For example, a security control might be filtering and directing traffic. See **Figure 11** and **Figure 12** in Section 4.4 for more information.

3.4.1 Assumptions: Personal Device Use Case

Due to the small size of some connected health devices they exist in an extremely constrained environment and therefore may require different security considerations than larger connected health devices with more computing capacity – such as monitors, scanners or even watches. From the constrained environment and drive to make IoT solutions tailored and user-friendly, it is assumed the hearing aid or similar devices will connect to another mobile device – such as a phone or tablet – or a personal and/or health-professional's computer for management and protection. Although it is noted that low power wireless technologies are a common connectivity solution for hearing aids, we make no assumptions related to the connectivity technologies used to connect these devices.

3.5 General Assumptions

3.5.1 Ownership

It is assumed that devices provided by the healthcare provider will be owned (or leased) by the healthcare provider and therefore the provider will have an appropriate degree of control over the device. Use case examples include the fixed MRI scanner, portable vital signs monitor and loaned blood pressure monitor.

It is assumed that personal devices such as hearing aids will be owned by the user, but may be serviced by the service provider or influenced by the healthcare provider. Third-party access controls may be supported and authorised by the patient, such as for a doctor to calibrate or configure the device. Healthcare providers may also request access to the patient's data, but will not have the ability to access that data without the appropriate consent.

3.5.2 Privileges

Devices owned by the healthcare provider may be accessed by authorised personnel – such as doctors or nurses – and temporary or specialised authorised users (e.g. specialist doctors and patients). Stakeholders and their related privileges will vary depending on the use case. This may include primary physicians, specialists, doctors and nurses in rolling shifts, the device/service provider, patients and their caregivers. Therefore, device configuration may include a range of access control cases, such as disallowing temporary users to time-constrained users.

We assume that a variety of access and administrative privileges will be managed by the provider and be dependent on various factors unique to that deployment. Privileges, including administrative privileges, are likely to be influenced by factors such as the ownership model, provider business model, criticality of the device to the user's health, sensitivity of data, location of the device within local area networks (e.g. high integrity zones), and capacity of the patient and/or their caregiver.

We also acknowledge that patients may have access to the devices' full functionalities, and should be given control of their own data to the extent possible. At the same time, patients do not have administrative privileges. For example, a patient should be able to make full use of a portable monitoring device, any related apps or services, and be able to share their data with select healthcare professionals. However, they may not be able to change the device configuration for data collection, administrative privileges or prevent updates.

3.5.3 Industry-Specific

As discussed in Section 2, the health industry is traditionally highly regulated. However, regulation has not yet caught up with changes in the health industry related to the IoT and security. Health-related IoT providers in certain industry sectors (e.g. medical grade devices) will likely have more regulation constraints than others (e.g. consumer IoT providers) in the near future, and so there will be a variance in security and audit requirements between classes of devices and products. We assume that the IoT provider will adhere to sector-specific requirements including regulations and best practices.

Regulation of health data confidentiality varies by country and, though out of scope for this document, it is highly recommended that relevant market regulation be reviewed by IoT providers. For example, since 1995, data protection regulations in Europe have defined health data as a “special category” [ref 3] of personal data that requires stricter conditions on its processing and a higher degree of security to protect it; this has been carried over into the current GDPR [ref 4]. In the US, although there is no general regulation protecting personal data, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 sets out requirements on health care providers for the privacy [ref 1] and security [ref 2] of health care records.

3.5.4 Technology Neutral

This reference architecture is intended to be technology agnostic, and therefore should be flexible and broadly applicable to health-related IoT deployments. It is important to keep in mind that the business models of IoT solutions, particularly device structures, and unique deployments and environments will all impact implementation of this architecture. Therefore, the paper provides a resource of examples and not a rigid implementation of the architecture described here. Where existing protocols or standards are referenced this is for illustration and they are not intended to be prescriptive references.

3.5.5 Network Technology

No assumptions related to device connectivity are made. This is for various reasons. For example, technology has evolved over time and many healthcare providers will be using both new and legacy devices. Additionally, connectivity capabilities depend on the specific device. For instance, upload is supported in older portable vital signs monitor models using RS232 serial ports for PCs or Infrared (IrDA) for PDAs. Recent models may include a variety of solutions such as mobile cellular, USB, broadband Internet (e.g. Ethernet or Wi-Fi) and Bluetooth connectivity. Considerations for communication between different network technologies are explored in Section 4.5, *Portable: Hybrid with Different Network Technologies*.

4 Reference Architectures

This section presents three network topologies ("bounded", "boundaryless" and "hybrid") and provides an environment map and network architecture for each. Discussions of relevant security concerns guide recommendations on where and how trust and security management features may be applied in each architecture to support good security practices. The best place to consider security risks is where data flow crosses a trust boundary. In these architectures, this often coincides with a network boundary. The bounded network topology can be used as the baseline example of how security management features can be implemented at trust boundaries to support layered security. The boundaryless and hybrid architecture models are necessarily linked to the bounded architecture where data crosses network boundaries (e.g. internal/external) and is shared between devices or subnetworks.

A "bounded" network topology has a defined boundary between network zones, either intentionally or not – such as gateways between secure networks or a bridge between network technologies. Security functions implemented at the boundary may protect devices, systems, or networks. This topology is particularly relevant to fixed IoT health devices and some portable device use cases.

A "boundaryless" network topology has no defined organisational intranet or security protections that may come with it. As a result, end-to-end security mechanisms are needed. Important security mechanisms to consider in a boundaryless environment include authentication and authorisation of device access. Using the trust boundary to ensure authorised accesses supports confidentiality and integrity of data. This network topology is particularly relevant to portable IoT health devices and some personal device use cases.

A "hybrid" network topology may include a variety of network technologies and topologies – including bounded and boundaryless networks. Health service providers may be more restricted as to where and how security features are implemented due to different ownership models. For example, a firewall between internal and external networks and traffic monitoring and routing capabilities might be the first available layer of security control for the health provider. This network topology is particularly relevant to portable and personal health devices.

Finally, some basic security considerations throughout the lifecycle and ecosystem of the IoT health device which are relevant but out of scope for this document are briefly discussed, in particular, platform security and compliance and certification.

4.1 Guide to the Reference Architectures

This section is divided into three network architectures: bounded, boundaryless, and hybrid. Each section includes two parts: the first is an environment mapping including example security management features, the second is a network architecture. Below is a brief overview of the information in each section.

Environment Mapping

Each environment mapping section includes a figure showing the data flow between elements in the architecture, directions of data flow, and where the flows cross trust boundaries. This includes internal and external points of information generation and sharing. In each use case a selection of weak points and recommended security features are highlighted for illustration but may apply to other use cases and are by no means exhaustive.

Network Architectures

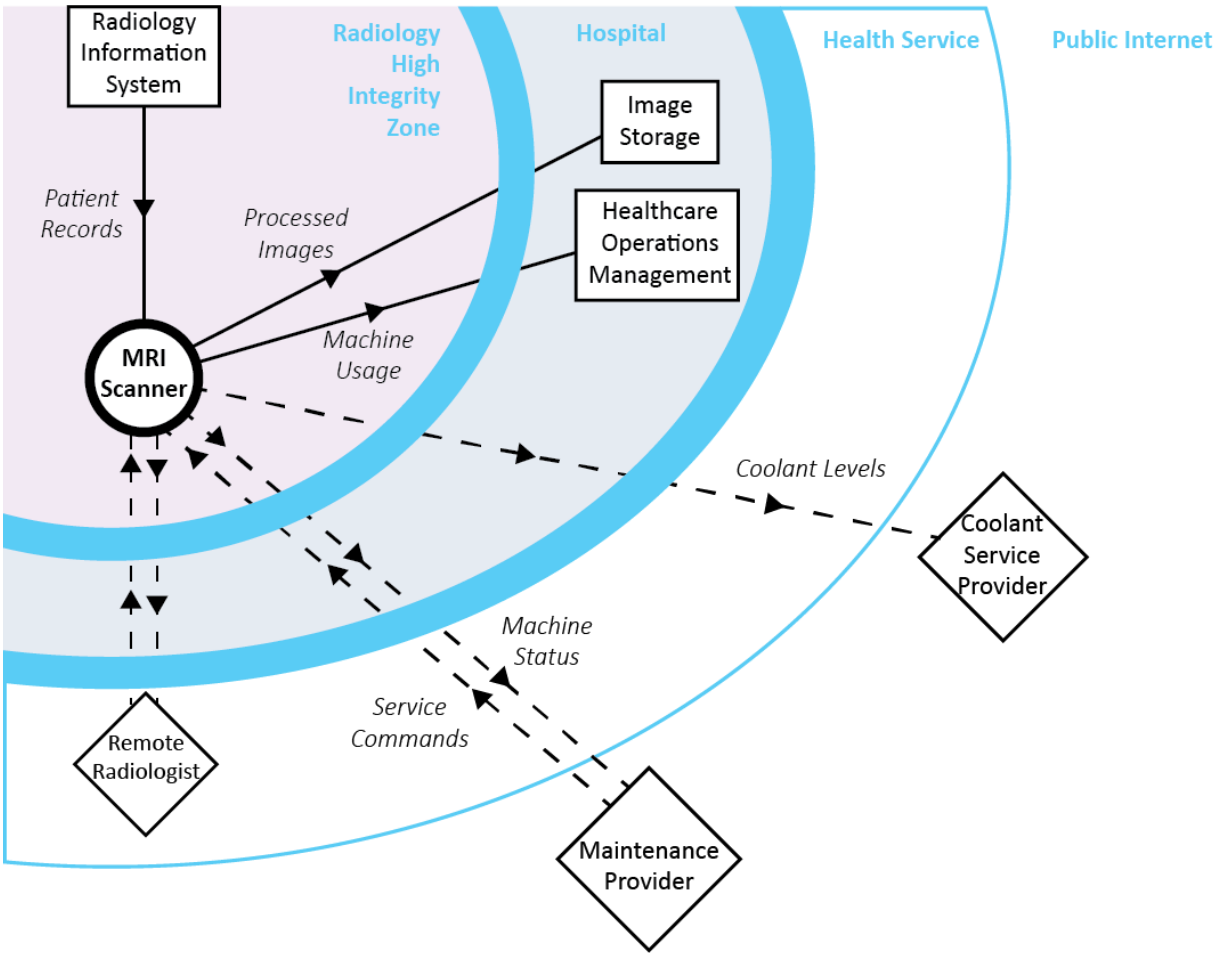
The sections on network architecture moves away from the detailed look at data flows and focuses on network boundaries and technologies.

4.2 Bounded Network with High Integrity Zone

A bounded network has a boundary between one or more network zones. Boundaries can be intentional (e.g. design) or necessary (e.g. using different network technologies). In either case, the boundary can provide a suitable place to implement security measures such as traffic controls. Using boundaries to segment networks helps to protect critical devices. It also supports good information security practices and compliance with data protection regulations by implementing additional safeguards for patient information. They can also be used to manage levels of trust assigned to different zones (e.g. high integrity radiology department versus general intranet). Using boundaries may minimise attack surface and allow for better device management. Boundaries that arise as a by-product of different network technologies may act as a gateway between bounded zones or other network technologies and support interoperability.

This topology is particularly relevant to fixed IoT health devices and some portable device use cases.

4.2.1 Bounded IoT Health Device Environment Mapping



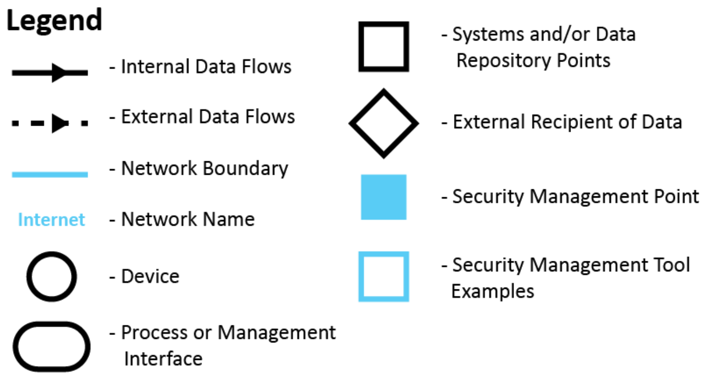

Legend
- Internal Data Flows
- External Data Flows
- Network Boundary
Internet - Network Name
- Device
- Process or Management Interface
- Systems and/or Data Repository Points
- External Recipient of Data
- Security Management Point
- Security Management Tool Examples

Figure 7: Bounded Network Map

The diagram above shows several nested zones, with the innermost high integrity zone containing the critical systems of the radiology department. This is contained within a hospital's intranet, which is itself part of a wider health service network (such as the "NHS Spine" in England). There are also data flows out to the public Internet, for communication with external machine maintenance and service providers.

There are several benefits of bounded environments. Boundaries allow for strong network security resources at points of interconnection. Boundaries also support layered security in an environment with a variety of devices ranging in capacity and criticality. For example, a security gateway may ensure availability of critical devices if part of a network is attacked by protecting the high integrity zone and its devices with low or poor security capacity from external threats.

Below are a few examples of security management features that may be implemented at the network boundaries:

- Separating internal and external networks to protect against incoming threats and enable the monitoring and segmenting of traffic as necessary
- Separating local networks into different network zones to better manage security based on the needs of that zone and to minimise attack surface for a network (e.g. protecting a high-integrity zone)
- The ability to provide alerts and notifications in the event of anomalies
- Communication with a database for device and/or identity management
- The ability to assign attributes and authorisations to a device and/or group of devices

4.2.2 Bounded Network Architectures

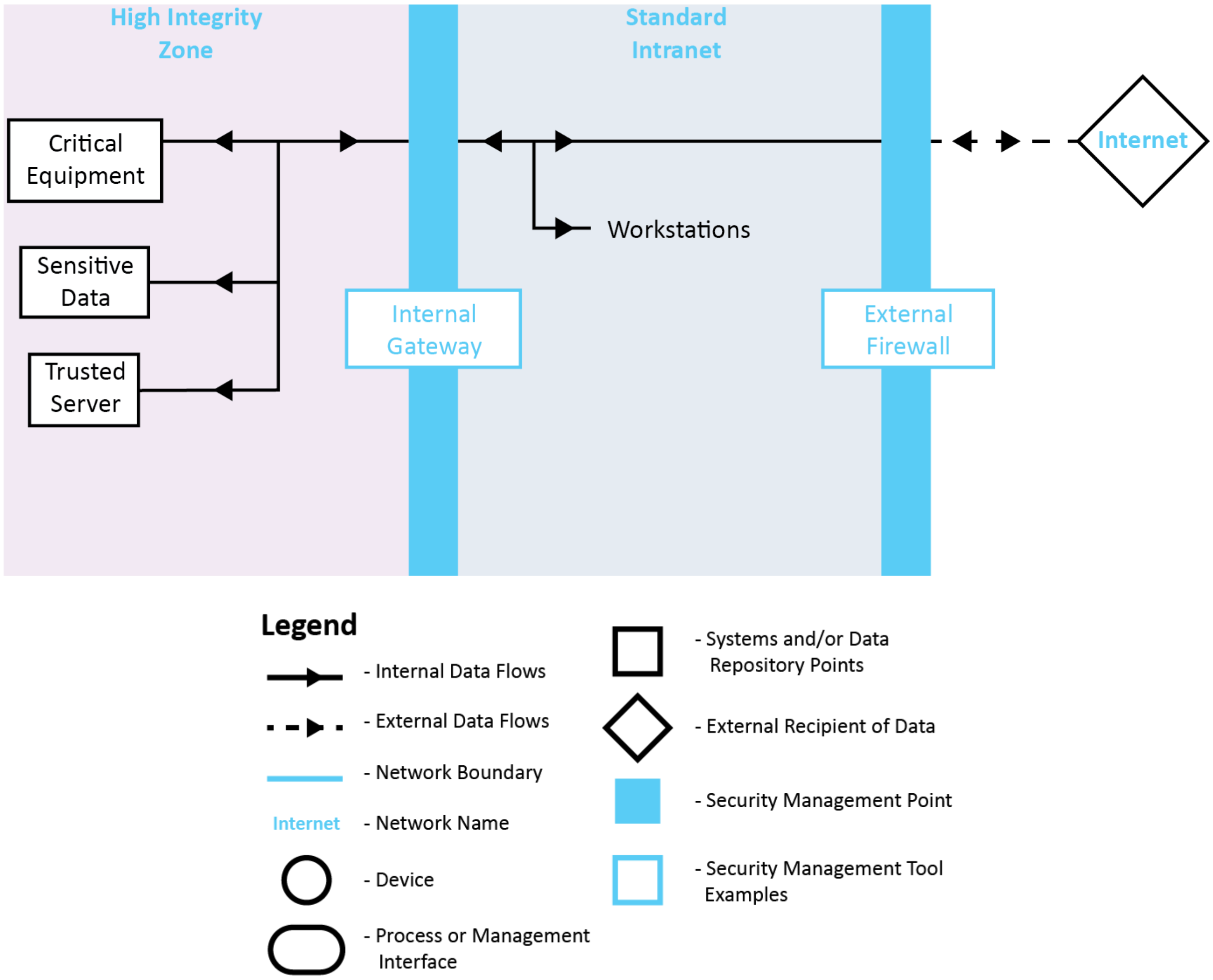


Figure 8: Bounded Network with Similar Network Technologies

The diagram above shows a network that has been segmented by design into separate zones with different security levels at least partially supported by a security gateway or firewall. For more information on the specific security concerns here, see the Fixed Use Case, and potentially the Portable Use Case, in Sections 3.1 and 3.2 respectively.

Some of the boundary functions are common – for instance, network segmentation. Some of the boundary functions may be specific to that use case. For example, network managers may want to allow only specific users and devices onto the high integrity zone intranet. This might include specialist technicians, doctors, and devices like the MRI scanner. Whereas those users and devices allowed to connect to the standard intranet are likely to be more in number and variety (general nurses and doctors, various hospital IoT health devices, etc.). Security functions implemented at specific points allow granularity of control and additional security within the local networks.

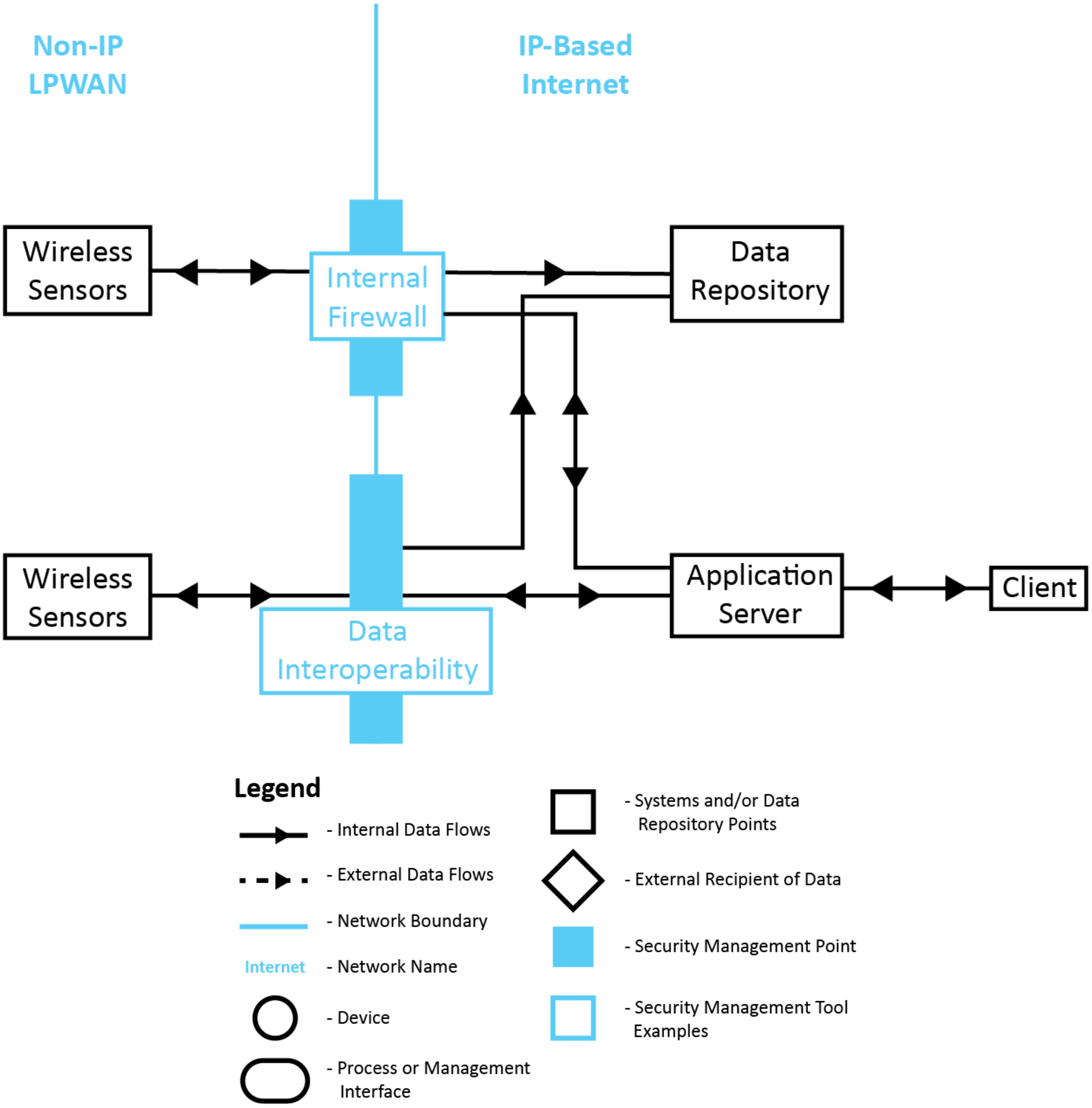


Figure 9: Bounded Network with Different Network Technologies

The diagram above shows a network that has distinct segments due to the devices on it using different network technologies requiring a gateway provided to bridge them. **Figure 9** is an example of how a necessary boundary (e.g. using different network technologies) presents an opportunity for layered security. For example, implementing a firewall at the network boundary may protect the networks and devices from external threats. Boundaries also present an opportunity to support interoperability between systems or devices. For instance, one network boundary in **Figure 9** is shown here including a data interoperability function.

4.3 Boundaryless Network

“De-perimeterisation” is a phenomenon that is widely recognised in enterprise network architectures which highlights the benefit of features such as access controls and managing updates. This is driven by trends including an increasingly mobile workforce, “bring your own device” and increasing use of Internet-based cloud services that provide advantages in the cost and agility of provisioning IT services. Similar trends can be seen in the health sector, where there is an increasing desire to provide services to patients outside of a traditional hospital or clinic environment, and similar advantages to be gained from the use of cloud services.

Another trend analogous to enterprise bring-your-own-device (BYOD) policies – including similar challenges to security – is clinicians making use of data from patients' own personal devices, such as connected hearing aids, to inform healthcare. Additionally, a clinician might have a role in configuring or managing patients' portable devices. When network nodes, such as workstations and servers, are no longer within a protected organisational intranet, end-to-end security mechanisms are required to authenticate and authorise access to devices, networks and data, as well as to provide confidentiality and integrity of boundaryless information flows. Because devices (e.g. a nurse's tablet computer) may change hands or users, end-of-life management and reconfiguration are also important elements to consider.

This network topology is particularly relevant to mobile IoT health devices and some personal device use cases.

4.3.1 Boundaryless IoT Health Device Environment Mapping

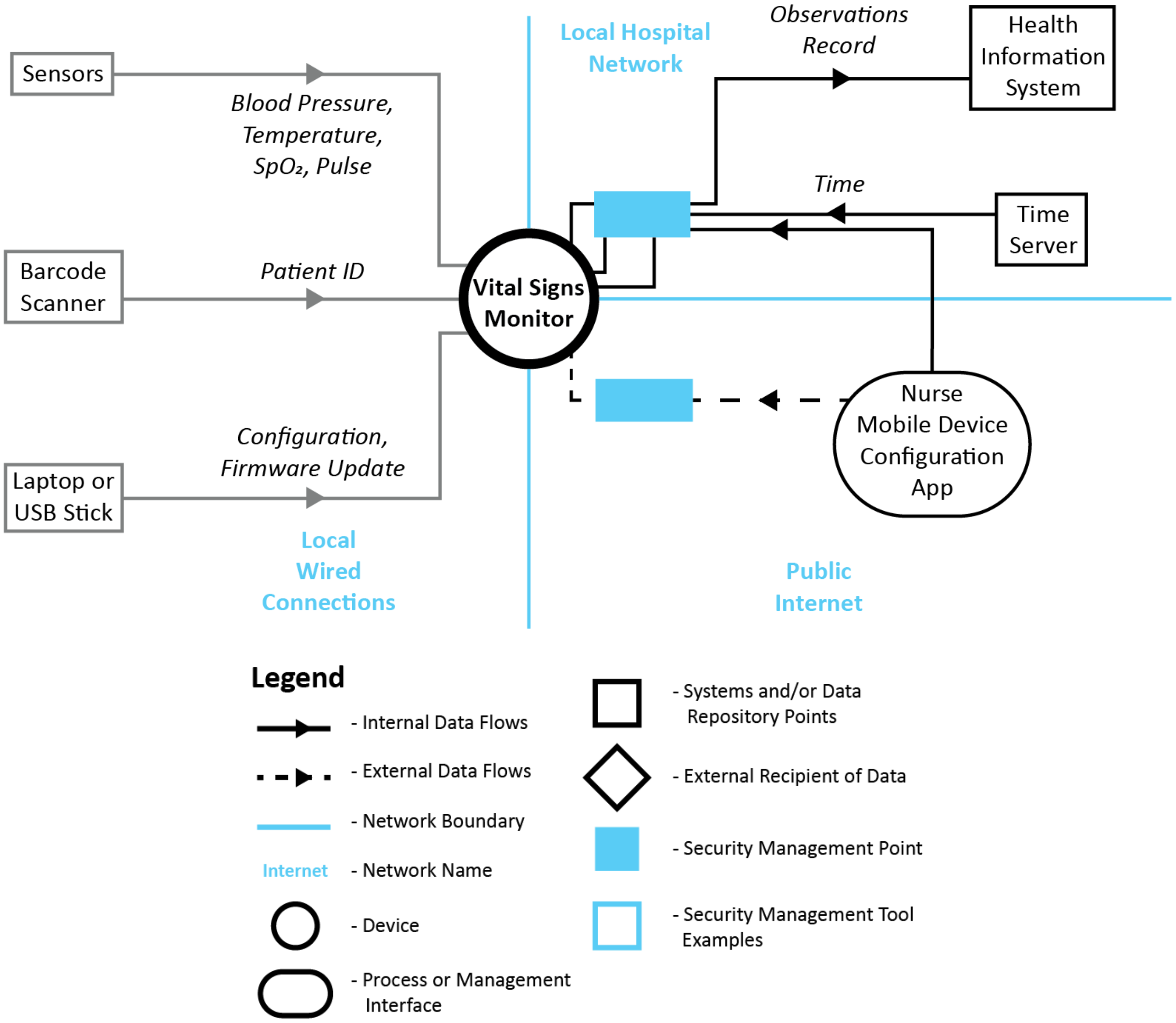

Sensors
Blood Pressure, Temperature, SpO_2, Pulse
Local Hospital Network
Observations Record
Health Information System
Time
Time Server
Barcode Scanner
Patient ID
Vital Signs Monitor
Configuration, Firmware Update
Laptop or USB Stick
Nurse Mobile Device Configuration App
Local Wired Connections
Public Internet
Legend
- Internal Data Flows
- External Data Flows
- Network Boundary
Internet
- Network Name
- Device
- Process or Management Interface
- Systems and/or Data Repository Points
- External Recipient of Data
- Security Management Point
- Security Management Tool Examples

Figure 10: Boundaryless Network Map

The diagram above shows three different networks – local wired or Wi-Fi accesses and public internet – that can connect healthcare devices, such as a vital signs monitor or a nurse's mobile device[6]. In effect, this is a boundaryless network architecture where communication can occur end-to-end over the public Internet and also switch between networks. For instance, the monitor is portable and can be plugged into any convenient Ethernet port or use public Wi-Fi. The nurse's mobile device may be able to connect to public Wi-Fi or use a cellular connection when "on location" and then connect to the local hospital network when working locally.

It is likely that security functions, such as updates or access controls, may need to be managed by the health provider over a local connection. Devices inside a health environment (such as a hospital or out-patient care facility) that are connected to the public internet pose additional risk to local networks due to the threat of transferring malicious content, such as malware, to the local network during data transfer.

The IoT devices themselves may lack additional layers of security (such as whitelists or intrusion detection), may be "findable" and traceable by those looking to exploit vulnerabilities, and at risk of participating in command and control type attacks such as distributed denial of service (DDoS). Therefore, IoT portable health devices should implement best practices and use a risk assessment to determine the appropriate security features, such as best practices in general IoT device security [ref 44]. For example, retaining "administrative" role-based access controls for IT managers instead of the user provides added oversight of features such as "guest" accounts, requirements for password access, and managing updates. Implementing a mobile device security management policy may also assist with implementation and management of security best practices but particulars are out of scope for this paper.

Below are a few examples of security management features that may be implemented at the security management points:

- A central point for authenticating devices may:
    - Carry out authentication processes
    - Act as a cache for authenticated devices
    - Store authentication credentials
    - Support varying levels of authentication (e.g. single token, server, and mutual authentication)
- A central point for authorising access to the network may:
    - Act as a device management tool to apply or revoke privileges
    - Support creation and enforcement of permissions lists (e.g. black- and whitelists)
    - Support trusted device/group identity management
- An authentication/authorisation tool may provide alerts if an authenticated device has been tampered, authorisation privileges have been modified, or is trying to execute unauthorised actions
- An authentication/authorisation tool should use at minimum best practices in password and cryptography systems to support authentication and authorisation processes
- A central point for managing device end-of-Life and re-configuration may:
    - Manage permissions and revoke authorisation
    - Understand what patient information (e.g. type or level of sensitivity) is accessible by the device and be able to protect this data as needed
    - Support data erasure – permanent deletion of settings, user account information etc.
    - Support decommissioning or transferring device identity
    - Support precautions for transferring device usage and re-configuration, such as data erasure, factory re-set, etc.

[6] Although wired connections are shown on the above diagram for completeness, they were excluded from the threat analysis, considering physically present threats to be out of scope.

4.3.2 Boundaryless Network Architectures

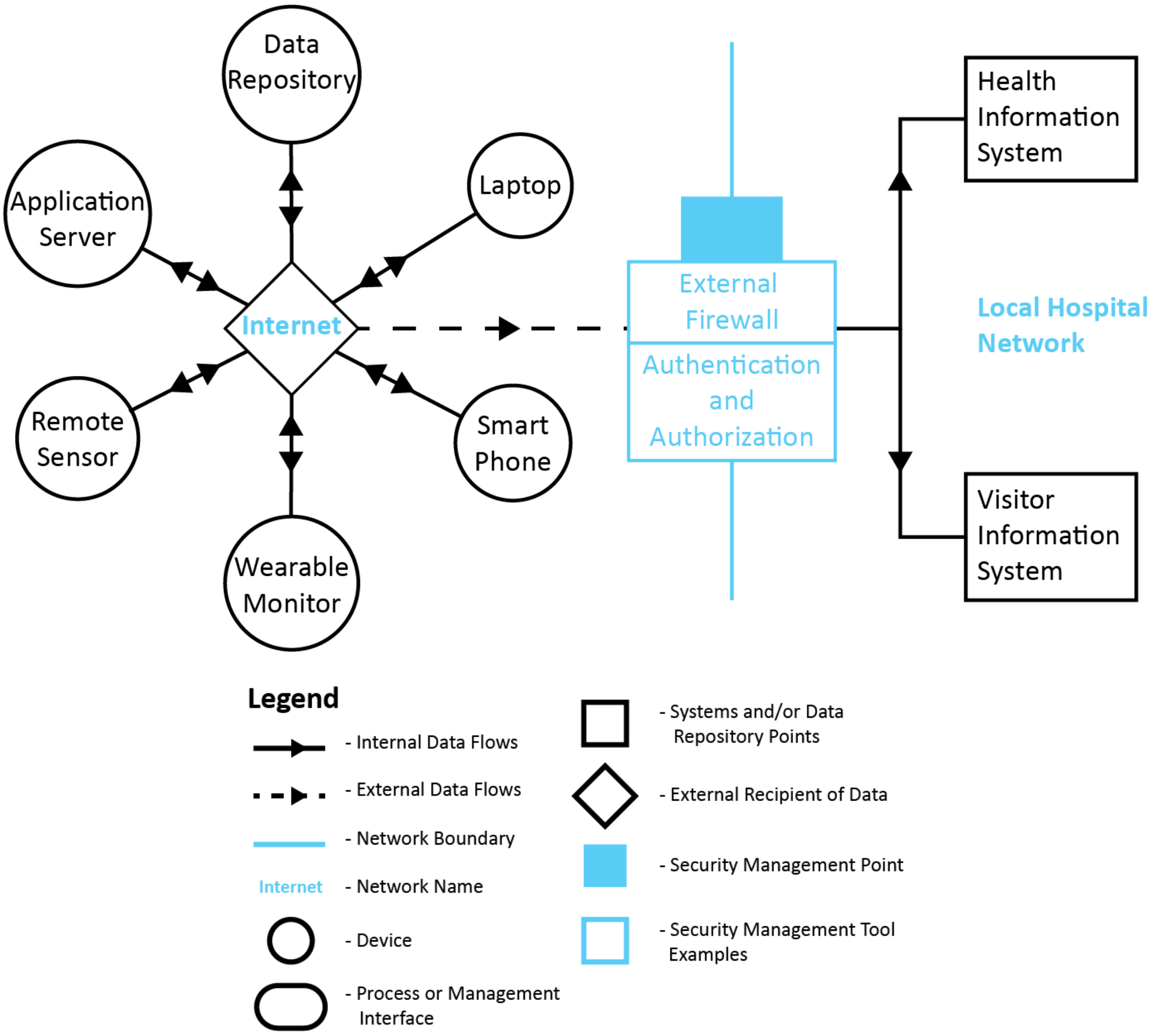

Data Repository
Application Server
Laptop
Internet
Remote Sensor
Smart Phone
Wearable Monitor
External Firewall
Authentication and Authorization
Health Information System
Local Hospital Network
Visitor Information System
Legend
- Internal Data Flows
- External Data Flows
- Network Boundary
Internet - Network Name
- Device
- Process or Management Interface
- Systems and/or Data Repository Points
- External Recipient of Data
- Security Management Point
- Security Management Tool Examples

Figure 11: Boundaryless Network

The diagram above shows a boundaryless network, where each of the nodes (devices, servers and repositories) has its own independent connection through the public Internet. All of the nodes communicate using IP, which may be tunnelled through various different bearers (cellular data, Wi-Fi, etc.)

Layers of security are particularly important in environments such as a boundaryless network. As noted above, there is an attack surface of the local area networks and devices themselves will vary in capacity. The extent to which the health provider owns/controls the device will also have an impact on the ease with which particular security controls (e.g. access and update controls) can be managed.

A key security management point in this environment is the point at which a device on public Internet connects to or communicates data to the local network. Using traffic monitoring and routing features on the local hospital network (e.g. a gateway) to direct traffic, authenticated users (e.g. remote healthcare professionals or patients) can be routed to appropriate internal networks. It is important to implement appropriate features at key points such as network boundaries and data or device access points to protect local networks, devices and data from incoming threats and unauthorised access. Where possible, data being sent from health service devices (e.g. physician laptops) must be communicated over secure networks such via a VPN when working remotely.

4.4 Hybrid with Different Network Technologies

Not all health-related IoT devices can communicate over IP-basted networks. Therefore, it is important to consider how different network technologies may interact in this space. This network topology is particularly relevant to portable and personal health devices, with the example architecture below focusing on a personal device use case (connected hearing aid). Relevance is dependent on the specific implementation and device capabilities. It is conceivable that a loaned device with an app on the user's mobile phone connects in a similar manner as the use case here.

It is important to note that this document does not attempt to specify or go into detail regarding a patient's personal device. Instead, the focus here is on the sharing of the patient's data with the healthcare provider and the tools that provider has to reduce risk to their internal systems' security when receiving that data. The consumer device market is a complex environment and this particular interface between consumer devices and healthcare warrants its own detailed examination.

4.4.1 Hybrid IoT Health Device Environment Mapping

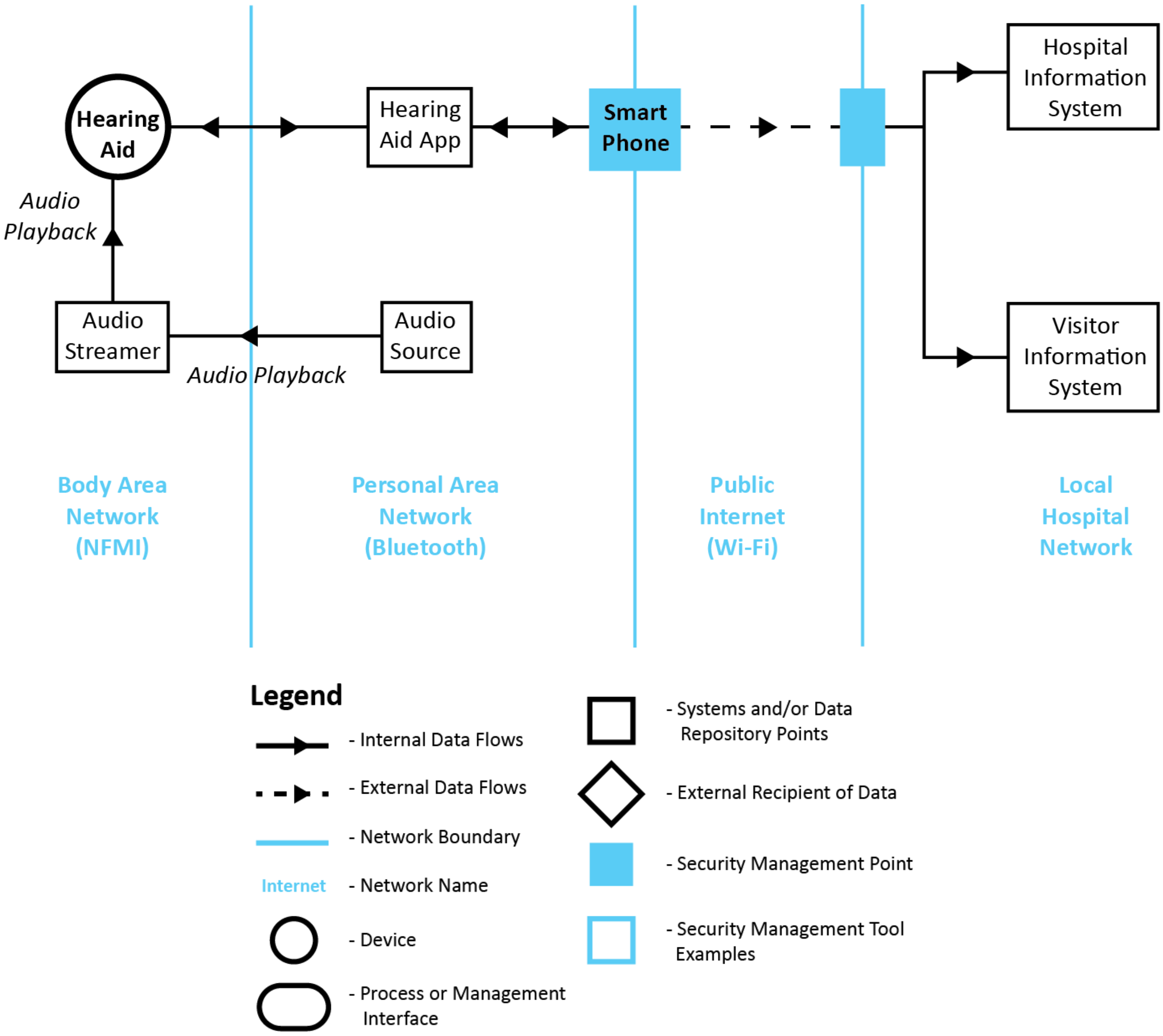


Figure 12: Hybrid Network Map

The diagram above shows an architecture with three different network technologies – IP over the Internet, a Bluetooth Personal Area Network (PAN)[7] using several profiles (not including IP), and a Body Area Network (BAN)[8] using Near Field Magnetic Induction (NFMI). These are shown on the diagram as three zones. The zones here are used to illustrate the network technologies that the different devices and services use to communicate with each other in this specific hybrid network example. However, it is important to note that adjacent zones do not necessarily have a logical boundary. The hearing aid may be fully exposed to the PAN, and the hearing aid App is fully exposed to the Internet (for example on a smartphone using public Wi-Fi). The hearing aid is however not directly exposed to the Internet because there is no direct routing between the BAN and the Internet, thus this is not a fully boundaryless network architecture.

The hearing aid itself will function in a constrained environment and therefore may not have the ability – or need – to implement some technical security techniques such as encryption or mutual authentication. The fact that it is not directly connected to the public Internet does support some level of security by minimising its attack surface; additionally, security attributes may be built into the communication protocol by default.

Devices may share data with the health service provider locally or remotely. Devices in this network architecture may be owned by a health service provider or privately owned by the patient. It is also conceivable that a user's smart phone may offer additional layers of assurance through basic security capabilities such as encryption or user authentication and authorisation. Although the specifications of a user's smart phone is out of scope for this document, this is an example of how a personal device may integrate into an architecture. This level of formal interaction is currently evolving and health service providers as well as developers may consider a variety of possible future solutions. For example, when communicating a patient's information to the health service provider, the phone and health system "talking" with each other should be mutually authenticated before information is shared.

Because a variety of data and devices will be connected to or communicated over the health provider's network, monitoring the network and managing authorisation are good risk mitigation techniques. Below are a few examples of security management features that may be implemented at the security management points:

- Reporting features for monitoring and audits, which may include:
  - A log of monitoring and audit activity
  - Access to past reports
  - Query options
- Features that enable further action as a result of monitoring and audit:
  - Controlling traffic flows and segmentation
  - Implementing anti-virus/malware solutions
  - Pushing updates or patches to devices
  - Audit and update roots of trust as necessary
- The ability to revoke authentication and/or authorisation to decommission devices or transfer ownership (e.g. manage device whitelists and/or blacklists)

[7] A Personal Area Network is a network that is within an individual's personal space, connecting devices around that person (e.g. mobile phones, computers, televisions, thermostats, etc).

[8] A Body Area Network is the network connectivity used by a wearable device (e.g. hearing aids, glasses, fitness trackers).

4.4.2 Hybrid Network Architectures

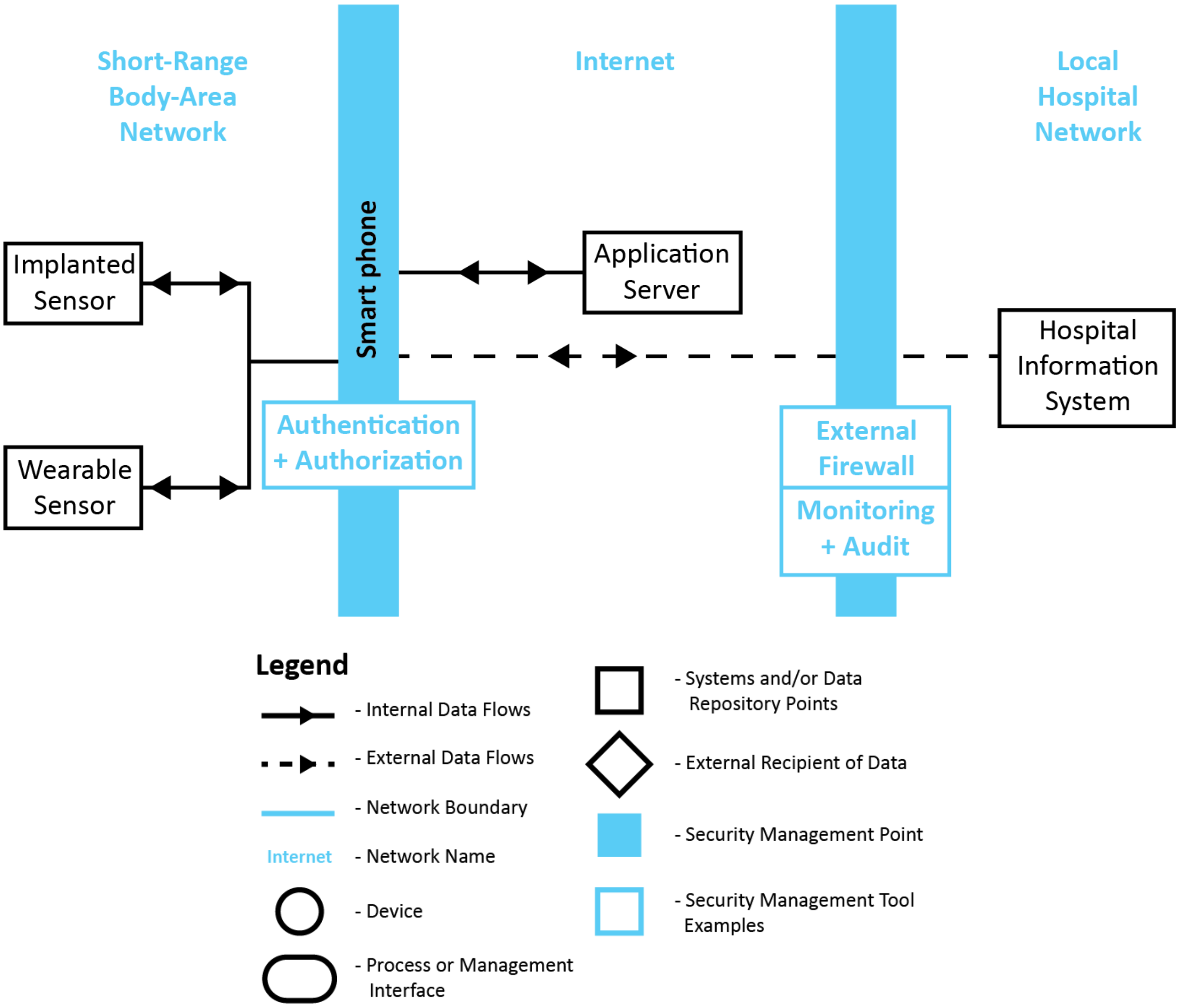

Short-Range Body-Area Network
Internet
Local Hospital Network
Smart phone
Implanted Sensor
Wearable Sensor
Application Server
Hospital Information System
Authentication + Authorization
External Firewall
Monitoring + Audit
Legend
- Internal Data Flows
- External Data Flows
- Network Boundary
Internet - Network Name
- Device
- Process or Management Interface
- Systems and/or Data Repository Points
- External Recipient of Data
- Security Management Point
- Security Management Tool Examples

Figure 13: Hybrid Network with non-IP segment connected to Cloud

Figure 13 shows a short-range communication Body Area Network (BAN) [ref 19] being used in conjunction with cloud-based services. When we include devices that are not themselves IP-capable in a system with cloud-based elements, we consider this to be a hybrid of bounded and boundaryless models. Non-IP-capable devices often have low power (in both computing and battery terms)[9] which also translates to limited security capabilities. However, the boundary offers a well-placed security management point and can act as an end point of a secure association. For example, security endpoint processing for the device can be offloaded to a gateway positioned at the boundary. However, there could be many solutions to this question, some of which are not yet developed. For example, in a household with many health-related IoT devices and need for on high-quality data, a patient may have a dedicated device, such as a loaned device, router or other networking device that incorporates these and other security-minded functions.

4.5 General Security Considerations for Health-related IoT Devices and Platforms

The security functions of health-related IoT devices and platforms is not a focus of this document. However, they are important factors that contribute to the overall security and safety of the ecosystem. Additionally, the risks associated with poor security in the health-industry are potentially serious – with the possibility of

[9] This is typically the motivation for the device manufacturer choosing not to support IP in the first place.

impacting user health and safety. Below, two important considerations for general health-industry IoT security are briefly discussed:

- Platform security and hardening
- Compliance and certification

4.5.1 Platform Security and Hardening

The threat analysis for this architecture considers attacks targeting the flow of application data, but it does not directly consider attacks against the supporting platform (middleware, operating system and hardware). Platform attacks are important because they are a common way in which systems are infected by malware. In some cases (e.g. ransomware or DDoS attacks) the attacker does not care about the data being processed by the attacked machine, but malware can also be used in a targeted way to subvert and bypass security controls implemented by applications (for example by installing a "rootkit" which the attacker can then use to get on to the platform and tamper with programs and data at a lower level).

Reducing the security risks of the platform is termed "hardening"; the need for hardening should be driven by a risk assessment[10] taking into account the value of the system, the protected assets as a whole, and specific deployment of a system (e.g. a small general practice with a few hundred patients or a large hospital with thousands of patients).

General purpose operating systems are very complex pieces of software with millions of lines of code, and typically have a continual sequence of security holes being found and patched. They are feature-rich and, in order to support a wide range of use cases, have many services enabled by default, a significant fraction of which will not be needed in any specific deployment – this means that a lot of attack surface may be being exposed for no particular benefit. One way to considerably reduce this attack surface is not to use a general purpose operating system (like Windows or Android) but to use a much less complex operating system designed for critical devices, usually a Real-Time Operating System (RTOS). This may however require more specialised development skills and more integration effort and cost, so the decision needs to be driven by the risk assessment mentioned above.

Whatever operating system is used, it is important to ensure that a currently supported version is used and that it is patched regularly. Unsupported operating system (OS) versions should not be used, if at all possible, due to increased threats and associated risks – these risks are significantly increase in a boundaryless architecture with increased external threats compared to that of a bounded network. If this is impossible (for example the system has legacy hardware components that will not work with current OS versions) then additional measures, such as those offered in this architecture, must be taken to isolate the device from potential attacks, using a tightly controlled network perimeter.

Services which are not needed should be turned off to reduce the attack surface, and platform security controls, such as whitelisting of applications, should be turned on. Security hardening guides are available for several popular platforms.

4.5.2 Compliance and Certification

Using standards compliance as a measure of security is not a complete solution, as compliance at any particular point in time is no guarantee against security flaws being found later. Still it is helpful, particularly for

[10] The STRIDE threat classification model was used for this threat analysis and risk assessment. There are variety of risk assessments that can be adopted based on the user's need. These include: PASTA, VAST, Trike, NIST's Cyber Security Framework, NCSC's Risk Management Guidance, ISO/IEC 27000 series (particularly those on information security risk management), and OWASP (application security). In particular, see the ISO process for risk management of networked medical devices [ref 20]. A solution provider should select the most appropriate model when executing an assessment.

procurement managers who do not have the resources to do their own full risk assessments (for example see the ISO process for risk management of networked medical devices [ref 20]) or to evaluate each of their vendors.

The IoT Security Foundation published an IoT Security Compliance Framework [ref 44] which includes a questionnaire which vendors can complete and thus provide their customers with increased assurance that their product includes good security controls.

The IoT Security Foundation also provides a Secure by Design Best Practice Guide aimed at product designers and developers with "advice on 'things to do' to help secure IoT products and systems" [ref 46]. Although it is focused on consumer products, many of the general principles apply to the IoT for health industry.

The US National Electrical Manufacturers Association (NEMA) also published a security questionnaire for use by medical device vendors, the Manufacturer Disclosure Statement for Medical Device Security (MDS^2). This can be used in conjunction with the ISO risk management process.

5 High Level Requirements

This section presents high level requirements aimed at achieving a minimum level of security when adopting the proposed architectures. These recommendations cover the use of encryption and digital signatures, authentication of data origin, design to anticipate and recover from denial of service, system hardening, management of vendors, and dealing with devices containing legacy components. This list should not be considered exhaustive and should be considered in conjunction with a risk assessment to understand the security requirements of each deployment.

- To protect patient privacy, tokenization of patient identity should be used in data stores where feasible.
- End-to-end encrypted data communications (typically TLS) should be used to preserve confidentiality for communications that cross the Internet, although where possible patient data should not cross the internet.
- Digital signatures should be used to preserve integrity. Highly sensitive data such as firmware updates should only be accepted from authenticated end points.
- Where possible, Denial of Service attacks should be mitigated by only accepting connection attempts from trusted network zones or specific IP addresses; where this is not possible, connection attempts should be rate limited [ref 47].
- Where data flows in both directions, the security context should be mutually authenticated and cryptographic mechanisms including encryption and signature verification should be bidirectional.
- System integrators must check that devices using encryption support compatible cipher suites which are sufficiently strong for the lifetime of the product or device.
- Where Denial of Service could impact patient care, communication bandwidth permitting the protocol should include confirmation of successful delivery of data and notifications, and a fallback process should be in place in the case of failed delivery.
- To minimise the attack surfaces, unneeded platform services should be turned off.
- Security controls should be enabled and only relaxed when there is a sufficiently low risk to do so[11].
- For safety-critical devices, consideration should be given to the use of less complex operating systems.
- Unsupported operating system versions should never be used in healthcare environments, both within both bounded and boundaryless architectures; if they have to be used, they must be placed in a protected network zone.
- Vendors should be evaluated and should demonstrate their use of secure development practices.
- Vendors should declare what security features they provide, and do so by complying with published criteria where available.
- When integrating systems from multiple vendors, customers should perform their own penetration testing.
- Intrusion Detection Systems should be considered, in order to reduce the time it takes to detect security breaches.
- Vendors should publish a vulnerability disclosure policy, and relevant information sharing bodies should be used to help manage their response to security breaches.
- Vendor fixes should be applied as soon as they become available.

[11] For example, the recent IETF initiative to use TLS for all web traffic: https://datatracker.ietf.org/meeting/83/materials/slides-83-iab-9-technical-plenary

6 References and Abbreviations

6.1 References

The following published sources have been referred to in the preparation of this document:

6.1.1 Applicable Privacy and Security Regulations

1. HIPAA, Title II, Privacy Rule
https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations
2. HIPAA, Title II, Security Rule
https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations
3. Article 8 of the EU Data Protection Directive 1995
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046
4. Article 9 of the EU General Data Protection Regulation 2016/679
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX:32016R0679

6.1.2 Medical Device Regulations

5. US FDA Device Advice: Comprehensive Regulatory Assistance
https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance
6. EU Regulation on Medical Devices 2017/745
https://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri=CELEX:32017R0745
7. How To Classify Your Medical Device, Lloyd's Register
http://info.lr.org/mdr
8. UK Government Criteria for Health App Assessment
https://www.gov.uk/government/publications/health-app-assessment-criteria/criteria-for-health-app-assessment
9. World Health Organisation, "Annex 1, GHTF Classification Rules" in *A Risk Based Approach for the Assessment of In Vitro Diagnostics (IVDs)*, 2014
http://www.who.int/diagnostics_laboratory/evaluations/140513_risk_based_assessment_approach_buffet.pdf
10. FDA, Mobile Medical Applications - Guidance for Industry and Food and Drug Administration Staff, 2015
https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf
11. FDA, Clinical and Patient Decision Support Software - Draft Guidance for Industry and Food and Drug Administration Staff, 2017
https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM587819.pdf

6.1.3 Health IT Architecture and Design

12. Security Architecture Design Process for Health Information Exchanges (HIEs)
https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7497.pdf
13. Personal Connected Health Alliance (PCHAlliance) Continua Design Guidelines
https://www.pchalliance.org/continua-design-guidelines
14. Fast Healthcare Interoperability Resources (FHIR)
https://www.hl7.org/fhir
15. Integrating the Healthcare Enterprise (IHE) IT Infrastructure Handbook: De-Identification
http://www.ihe.net/Technical_Frameworks/#IT
16. Atos IT Reference Architecture for Healthcare, 2011
https://atos.net/wp-content/uploads/2016/06/atos-itah-architecture-for-healthcare-whitepaper.pdf

17. B. W. Johnson and J. H. Aylor, "Reliability and Safety Analysis in Medical Applications of Computer Technology" in *Proceedings of the Symposium on the Engineering of Computer-Based Medical Systems*, 1988
https://www.computer.org/csdl/proceedings/ecbs/1988/4863/00/00005453.pdf
18. Kolkowska et al., "Information Security Goals in a Swedish Hospital" in *Proceedings of IRIS 31 - 31st Information Systems Research Conference in Scandinavia*, 2008
https://www.researchgate.net/publication/252258774
19. G.V. Crosby et al., "Wireless Body Area Networks for Healthcare: A Survey" in *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, vol.3, no.3, June 2012
http://aircconline.com/ijasuc/V3N3/0612asuc01.pdf
20. ISO/IEC 80001 Application of Risk Management for IT Networks Incorporating Medical Devices
https://www.iso.org/standard/44863.html

6.1.4 Technology Demonstrators, Test Beds and Reference Projects

21. Technology Integrated Health Management (TIHM) for Dementia
https://www.sabp.nhs.uk/tihm
22. Open Artificial Pancreas System (OpenAPS)
https://openaps.org
23. MedMinder makes Medication Smarter with IoT Connected Pill Box
https://www.gemalto.com/m2m/customer-cases/smart-pill-dispenser
24. J. Paul Finn et al., "MR Imaging with Remote Control: Feasibility Study in Cardiovascular Disease" in *Radiology*, November 2006
http://heart.ucla.edu/workfiles/Adult_Congenital/15MRImaging.pdf
25. J. Galster et al., "Do Wireless Hearing Aids Present a Health Risk?" in *Hearing Review*, June 2017
http://www.hearingreview.com/2017/06/wireless-hearing-aids-present-health-risk
26. J. Galster, "Making Sense of Modern Wireless Hearing Aid Technologies" in *ENT & Audiology News*, Nov/Dec 2014
https://www.entandaudiologynews.com/media/4032/entnd14-galster-new.pdf
27. L.B. Smith et al., "Connected Care: Reducing errors through automated vital signs data upload" in *Computers, Informatics, Nursing*, 2009
https://www.ncbi.nlm.nih.gov/pubmed/19726926

6.1.5 Reports and Surveys

28. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," in *IEEE Access*, vol. 3, pp. 678-708, 2015
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7113786
29. J. J. P. C. Rodrigues *et al*., "Enabling Technologies for the Internet of Health Things," in *IEEE Access*, vol. 6, pp. 13129-13141, 2018
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8246498
30. *Cyber safety and resilience: strengthening the digital systems that support the modern economy,* Royal Academy of Engineering, section 5 "Connected health devices"
https://www.raeng.org.uk/publications/reports/cyber-safety-and-resilience
31. NHS England, Lessons Learned Review of the Wannacry Ransomware Cyber Attack
https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf
32. HL7 Standards and Components to Support Implementation of the European General Data Protection Regulation, Mense and Blobel, 2017, European Journal for Biomedical Informatics 13 (1), pp. 27-33
https://epub.uni-regensburg.de/36600
33. NEMA/MITA White Paper CSP 1-2016, Cybersecurity for Medical Imaging
https://www.nema.org/Standards/Pages/Cybersecurity-for-Medical-Imaging.aspx

34. BSI White Paper, Cybersecurity of Medical Devices
https://www.bsigroup.com/en-GB/medical-devices/resources/whitepapers/Cybersecurity_of_medical_devices
35. US Department of Health and Human Services, Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA
https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf
36. IoT Privacy Forum, Clearly Opaque: Privacy Risks of the Internet of Things
https://www.iotprivacyforum.org/wp-content/uploads/2018/06/Clearly-Opaque-Privacy-Risks-of-the-Internet-of-Things.pdf
37. Brian Donohue, “Connected Medical Devices Simultaneously Increase Risk and Safety” in Threatpost, 2014
https://threatpost.com/connected-medical-devices-simultaneously-increase-risk-and-safety
38. Dana Ford, “Cheney's defibrillator was modified to prevent hacking”, CNN, 2013
https://edition.cnn.com/2013/10/20/us/dick-cheney-gupta-interview

6.1.6 Security Engineering (General)

39. NIST Special Publication 800-160, Volume 1, Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
https://doi.org/10.6028/NIST.SP.800-160v1
40. U.S. Department of Homeland Security, Strategic Principles for Securing the Internet of Things (IoT)
https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf
41. NIST Special Publication 800-121, Revision 2, Guide to Bluetooth Security
https://doi.org/10.6028/NIST.SP.800-121r2
42. IoT Security Foundation, Vulnerability Disclosure Best Practice Guidelines release 1.1, 2017
https://www.iotsecurityfoundation.org/best-practice-guidelines
43. BSIMM for Vendors (vBSIMM)
https://www.bsimm.com/about/bsimm-for-vendors.html
44. IoT Security Foundation, IoT Security Compliance Framework release 2.0, 2018
https://www.iotsecurityfoundation.org/best-practice-guidelines
45. IoT Security Foundation, “Make it safe to connect: Establishing principles for Internet of Things Security”
https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf
46. IoT Security Foundation, “Secure Design Best Practice Guides”, Release 1.2.1:
https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/Best-Practice-Guides-Release-1.2.1-December-2018_final.pdf
47. UK National Cyber Crime Security Centre “Denial of Service (DoS) guidance. Guidance to help organisations understand and mitigate against DoS attacks.”:
https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

6.1.7 Published Standards

48. ISO/IEEE 11073 Health informatics – Medical / health device communication standards
49. ISO/HL7 27931 Data Exchange Standards -- Health Level Seven
https://www.iso.org/standard/44428.html
50. ISO/TS 25237 Health informatics – Pseudonymization

https://www.iso.org/standard/63553.html
51. BSI, “The history of medical device legislation and clinical trials” in *A Guide to European Medical Device Trials and BS EN ISO 14155*, 2012
https://shop.bsigroup.com/upload/Shop/Chapters/BIP_0113_Medical_Device_Trials_SamplePages.pdf

52. ISO/IEC 27001 International standard "Information security management systems (ISMSs)" https://www.iso.org/standard/54534.html

6.1.8 Other References

53. World Health Organisation Constitution, 1946 http://www.who.int/governance/eb/who_constitution_en.pdf
54. IETF, "Key words for use in RFCs to Indicate Requirement Levels": https://www.ietf.org/rfc/rfc2119.txt
55. US Food and Drug Administration, "Digital Health": https://www.fda.gov/medicaldevices/digitalhealth
56. WHO "mHealth: New horizons for health through mobile technologies": https://www.who.int/goe/publications/goe_mhealth_web.pdf
57. Department of Health and Social Care, NHS Improvement, NHS England "Lessons learned review of the WannaCry Ransomware Cyber Attack": https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf
58. IoT Security Foundation "IoT Cybersecurity: Regulation Ready": https://www.iotsecurityfoundation.org/best-practice-guidelines
59. IoT Security Foundation "IoT Security Architecture and Policy for the Home -a Hub Based Approach": https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf
60. IoT Security Foundation "IoT Security Architecture and Policy for the Enterprise -a Hub Based Approach ": https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Security-Architecture-and-Policy-for-the-Enterprise-a-Hub-Based-Approach.pdf
61. Saltzer and Schroeder's 1975 paper, "The Protection of Information in Computer Systems" https://www.cs.virginia.edu/~evans/cs551/saltzer

6.2 Definitions and Abbreviations

API	Application Programming Interface
Botnet	A coordinated collection of Internet-connected devices infected with malicious software and controlled without the device owner's knowledge
BSI	British Standards Institution
DoS	Denial of Service Interruption to an authorised user's access to a digital resource, typically with malicious intent.
EU	European Union
FDA	US Food and Drug Administration
GDPR	General Data Protection Regulation EU regulations regarding privacy of personal data, came into effect in May 2018.
HIPAA	Health Insurance Portability and Accountability Act US legislation enacted in 1996, includes provisions in Title II for "Preventing Health Care Fraud and Abuse", applies to defined healthcare providers and their business associates.
HL7	Health Level 7 A set of standards for health data interchange, "Level 7" referring to the application layer of the OSI model.
HSP	Headset Profile (Bluetooth)
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol Protocol for routing packet data between network nodes, part of the Internet protocol suite. For

	two devices to communicate end-to-end over the Internet, they must each have IP addresses.
IrDA	Infrared Data Association
ISO	International Organization for Standardization
LAN	Local Area Network
Malware	Malicious software Software which hides harmful functionality under a legitimate-seeming façade (“trojans”) or which attaches itself to other legitimate software (“viruses”) and/or which seeks to infect other targets by exploiting security vulnerabilities (“worms”)
m-health	Mobile health Hardware and software applications for health using mobile data connections
MRI	Magnetic Resonance Imaging
NIST	US National Institute of Standards and Technology
OS	Operating System
OSI	Open Systems Interconnection An ISO standard conceptual model defining 7 layers of communications protcols, from the application layer down to the physical layer.
PC	Personal Computer
PDA	Personal Digital Assisant A pocket computer.
PII	Personally Identifiable Information
RFID	Radio-Frequency Identification
TLS	Transport Layer Security An IETF protocol providing integrity and confidentiality controls using cryptographic cipher suites.
UK	United Kingdom
US	United States of America
USB	Universal Serial Bus

Annex A - Starting Points to Understand Risk

Connecting medical devices to the Internet inevitably exposes them to cybersecurity risks and increases the threat to internal systems and networks (e.g. local intranets) as well as patients. Healthcare providers deploying IoT for health will require a good understanding of the related risks and adoption of good security practices. This document primarily considers the risks to information security and/or physical safety associated with compromised health-related IoT. **Figure 14** below is an example of how perceived risk may be categorised:

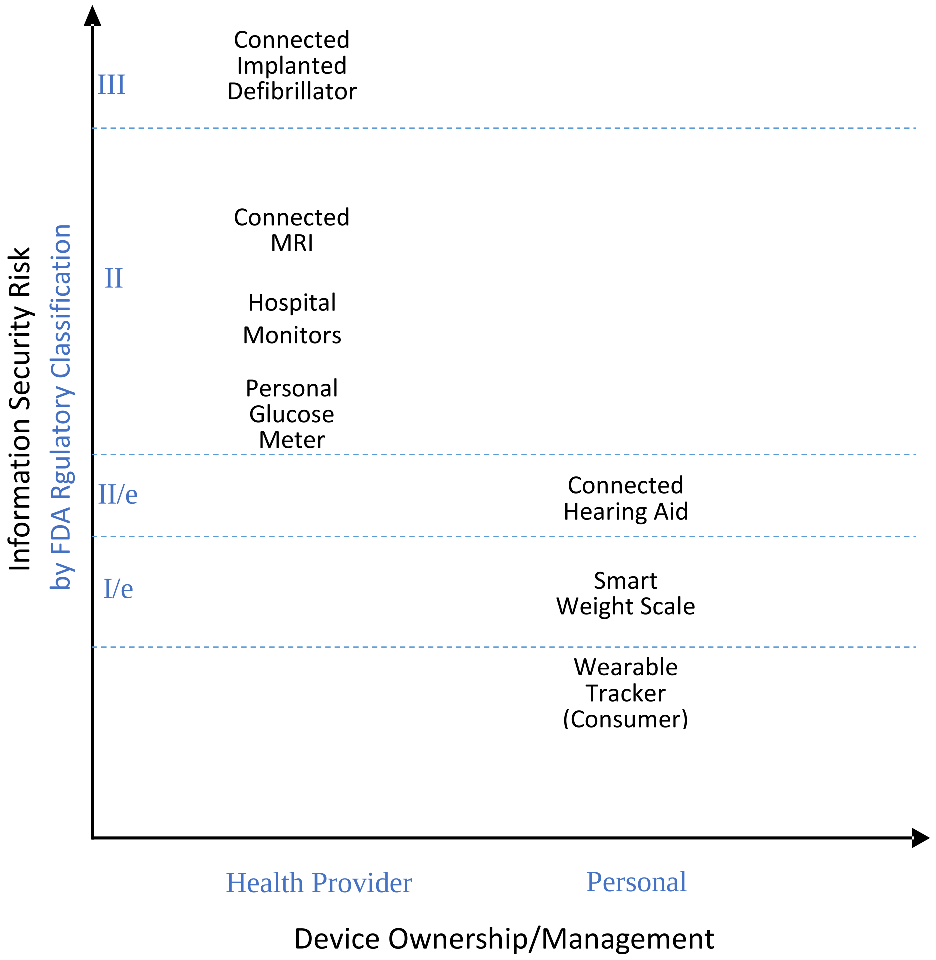

Information Security Risk
by FDA Rgulatory Classification
III
Connected Implanted Defibrillator
II
Connected MRI
Hospital Monitors
Personal Glucose Meter
II/e
Connected Hearing Aid
I/e
Smart Weight Scale
Wearable Tracker (Consumer)
Health Provider
Personal
Device Ownership/Management

Figure 14: Health-related IoT Devices and Information Security Risk

It should be noted that **Figure 14** is for illustration only. Perceived risks are correlated here with the FDA medical device classification [ref 5] scheme, which sets out the level of regulatory requirements for different classes of health devices to assure safety and effectiveness. This, for example, is why a consumer-grade wearable tracker is listed outside the purview of FDA regulation and not included in an FDA classification category. However, the wearable tracker may be subject to other consumer-focused and market regulations.

While the FDA classification may not map directly to information security risk in every case, such a framework can be used as a general starting point in risk assessment[12]. The actual assessment of regulatory classification and information security risk should be done on a by-device, per-case basis. This is due to a variety of factors such as physical size, computing power (e.g. ability to support encryption), and management interface (e.g. user interface or mobile app controlled), and direct or indirect impact on healthcare (e.g. MRI scanner versus surgical robot) that will affect the security risks posed by a health-related IoT device.

[12] For an example of a more detailed risk assessment, please see Annex B.

Annex B – Use Cases

B1. Fixed Use Case: Connected MRI Scanner

With modern technology, there are several reasons for wanting to add network connectivity to devices such as an MRI scanner, such as:

- Image Transfer & Storage

  DICOM (Digital Imaging and Communications in Medicine) is a data format and communications protocol enabling interoperable image transfer, and PACS (Picture Archive and Communication System) is a standard for storing, retrieving, presenting and sharing digitised medical images. Equipment supporting these standards allows clinicians and specialists using different IT systems to easily share scan results and thus provide quicker and better diagnosis.

- Remote Imaging & Control

  Enabling a remote expert to view and control MRI operation in real time has been shown to significantly improve the quality of results for specialist MRI procedures [ref 24].

- Consumable Monitoring

  MRI machines contain superconducting electromagnets which require cooling to extremely low temperatures. The cooling process typically uses helium, some of which may boil off in normal use, so more must be added from time to time. Helium is rare and expensive, so companies offer service contracts to regularly monitor levels and provide fills when necessary. Remote monitoring is more cost-effective and allows more frequent monitoring than would be feasible with on-site visits.

- Remote Management

  As for other large complex machinery, there is a trend to provide remote monitoring, predictive maintenance, and remote diagnostics to increase reliability and maximise uptime.

- Capacity Planning

  MRI scanners are very expensive pieces of equipment, and to maximise usage they are often located in shared facilities used by multiple healthcare organisations. Remotely accessible data on usage patterns can be used by capacity planners to optimise scheduling.

B2. Mobile Use Case: Wireless Connected Hearing Aids

With modern technology, there are several reasons for wanting to use wireless connected hearing aids, such as:

- Operating Controls From Mobile Device

  Several hearing aid vendors provide apps which allow volume, microphone patterns and other operating parameters to be controlled from a smartphone or tablet, being much easier to use than controls on the hearing aid itself.

- Remote Hearing Care

  Modern hearing aids have a sophisticated range of parameters that can be configured to suit different types and degrees of hearing loss, as well as different environments. Many of these parameters are not intended to be adjusted by the user, and they may need to be altered as a user's hearing loss progresses. Instead of requiring in-person visits to a professional audiologist, vendors are now providing apps that enable remote consultations and installation of new parameters, making the process more convenient and facilitating more frequent optimisation of hearing aid performance.

- Use As Mobile Phone Headset

  It can be awkward to use a separate Bluetooth phone headset while wearing a hearing aid, so it would seem useful to incorporate the phone headset functionality into the hearing aid itself. Many connected hearing aids use the Bluetooth Low Energy (BLE) technology because of their limited battery capacity, and BLE does not support the Bluetooth headset profile[13] (HSP), but with recent advantages in power management, hearing aids supporting full Bluetooth and the HSP have become available.

- Playback of Audio Sources

  Analogue coupling of hearing aids with audio sources has been available for some time using induction loops (often found in public facilities) or analogue radio; digital connectivity may now be provided using Bluetooth (with the same caveats as for the headset use case above) [ref 26]. Connection of hearing aids direct to TVs, music systems and other audio sources can enhance the listening experience for the user as it bypasses any ambient noise and provides more clarity

[13] One reason seems to be significantly increased latency in BLE audio compared to "full fat" Bluetooth. At the time of writing there are no official audio profiles for BLE, although Apple use their own custom modifications to the protocol.

- Monitoring Of Battery Levels

  The ability to display battery levels on a mobile device can give the user early warning of the need to change batteries. Some vendors also enable automatic notification to a caregiver, via SMS or email, that batteries are running low.

- Linkage To Home Automation

  One hearing aid vendor provides connectivity to a cloud service which links into home automation systems controlling lights, alarms, thermostats and so on. The hearing aid is both an input device (notifying the service when turned on or off) and an output device (playing back spoken alerts when someone rings the doorbell, for instance). This avoids the need to carry a separate device for any of these functions.

- Linkage To External Microphones

  Connecting via Bluetooth to external microphones instead of hearing aid loops – higher audio fidelity, longer range, auto connects via BTLE without user intervention.

B3. Portable Use Cases: Hospital Vital Signs Monitor and Blood Pressure Monitor

With modern technology, there are several reasons for wanting to use a portable monitors, such as:

- Automatic Data Upload

  The widely used HL7 standard [ref 49] defines data formats for many elements of an Electronic Health Record (EHR). Sensor devices, including vital signs and blood pressure monitors, are able to upload readings to a Health Information System where it automatically forms part of a patient’s medical records, avoiding risks of human error in transcribing readings. For example, the associated patient ID can be input from a patient’s wristband using an optical barcode or RFID tag to further reduce risks of transcription errors.

- Configuring Settings

  The settings on a modern health monitors can be quite sophisticated, including parameters which control the frequency of observations and rules specifying combinations of conditions which should generate alarms, and need to be configured differently for each patient. Some monitors allow download of configuration files prepared on a laptop or PC, providing improved ease of use compared to the limited interface available on the monitor itself.

- Time Synchronisation

  Some monitors allow synchronisation with a network time server or application for accurate time stamping of records, avoiding any problems due to incorrectly set or drifting internal clocks.

- Firmware Update

  As for any connected device which includes sophisticated firmware, periodic updates are required, to add functionality, fix bugs and patch security vulnerabilities.

IoT Security Foundation

www.iotsecurityfoundation.org