UNIVERSITÀ
DEGLI STUDI DI TRIESTE

dipartimento
di ingegneria
e architettura

Corso di Laurea in Ingegneria Clinica e Biomedica
Insegnamento di
Insegnamento “C.I. Informatica Medica”– 15CFU-365MI
Insegnamento «Complementi di Informatica Medica» - 6CFU-365MI-2

DATA PROTECTION AND CYBERSECURITY IN eHEALTH SYSTEMS

Prof. Sara Renata Francesca Marceglia

Why medical data are critical

BANKING

Data OWNER		Data USER
Bank account holder	=	Bank account holder

MEDICINE

Data OWNER		Data USER
Patient	≠	Healthcare professional

In medicine the owner of data does not have the knowledge to use it → data have to be shared with others

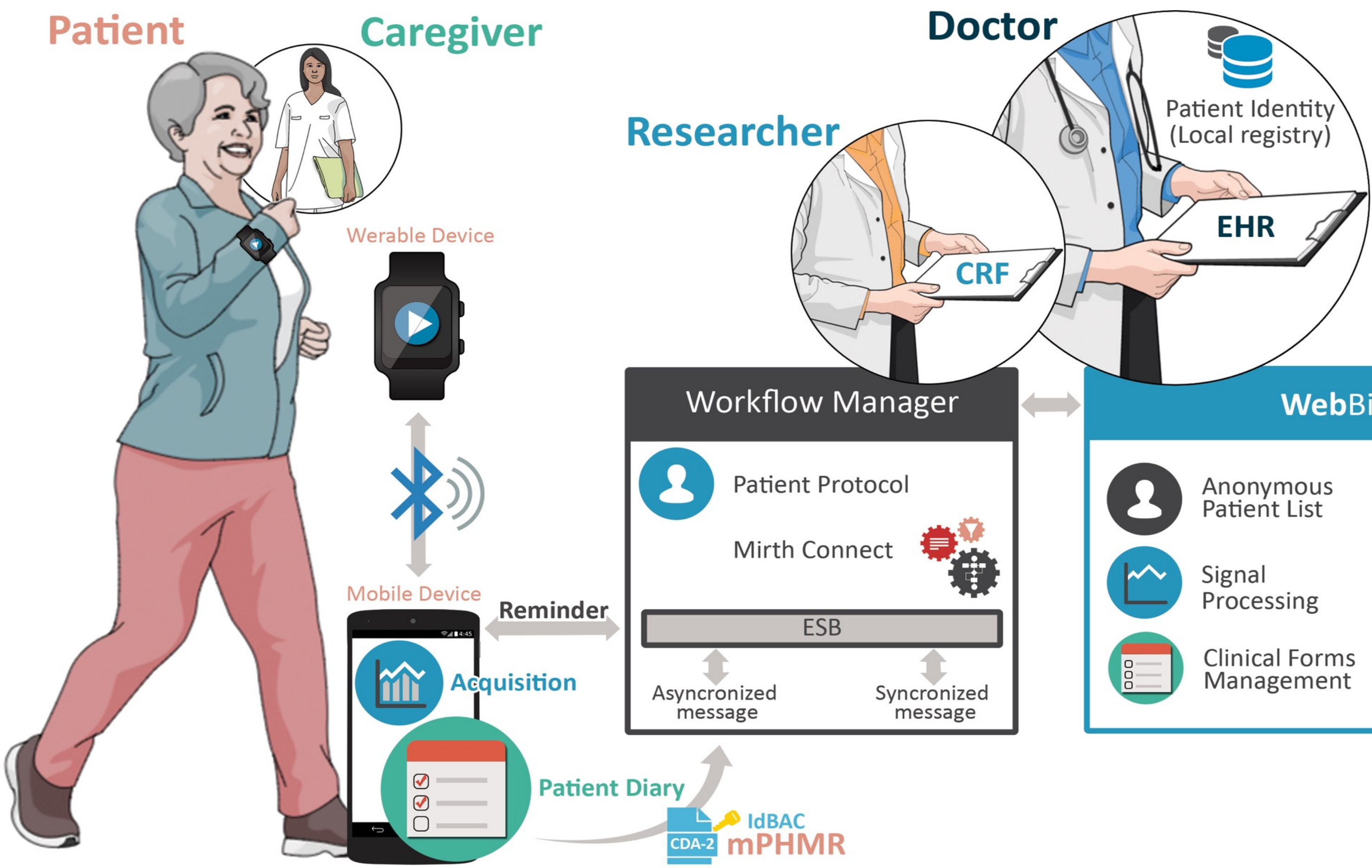
SHARED CARE

Shared care =

«A continuous and coordinated activity of **different persons in different institutions** under employment of different methods at different times in order to be able to help patients optimally with respect to their **medical, physiological, an social being**»

Data sharing and system integration is required to allow all the healthcare team to ensure **continuity of care.**

Complex scenarios



- Data transmission over different networks
- Data storage
- Multiple access to the system

Types of software

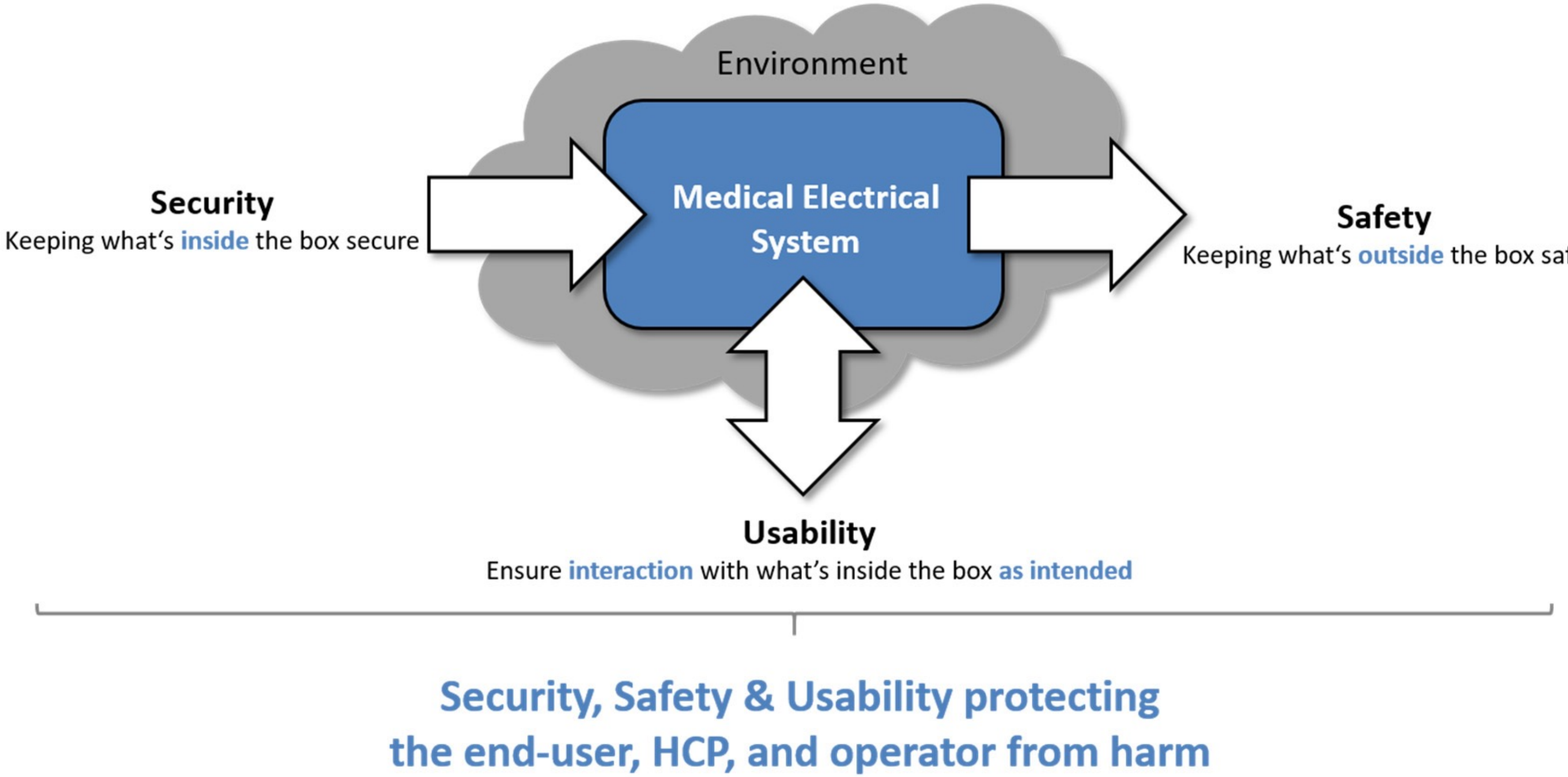
Software as accessory to medical device

- ‘accessory for a medical device’ means an article which, whilst not being itself a medical device, is intended by its manufacturer to be used together with one or several particular medical device(s) to specifically enable the medical device(s) to be used in accordance with its/their intended purpose(s) or to specifically and directly assist the medical functionality of the medical device(s) in terms of its/their intended purpose(s);

Software as medical device (SaMD)

- The term “Software as a Medical Device” (SaMD) is defined as software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device

Security, Safety, and usability in complex systems



From: ISO/IEEE 11073-40102:2022(E)

Software quality

- The software should **perform its intended functions** to meet its intended use (requirements)
- The software is **safe** (does not create injury or damage to the patient)
- The software provides a reasonable level of **availability, reliability, and correct operation**;
- The software is reasonably secure from **cybersecurity** intrusion and misuse.

General approach to software quality

Risk assessment

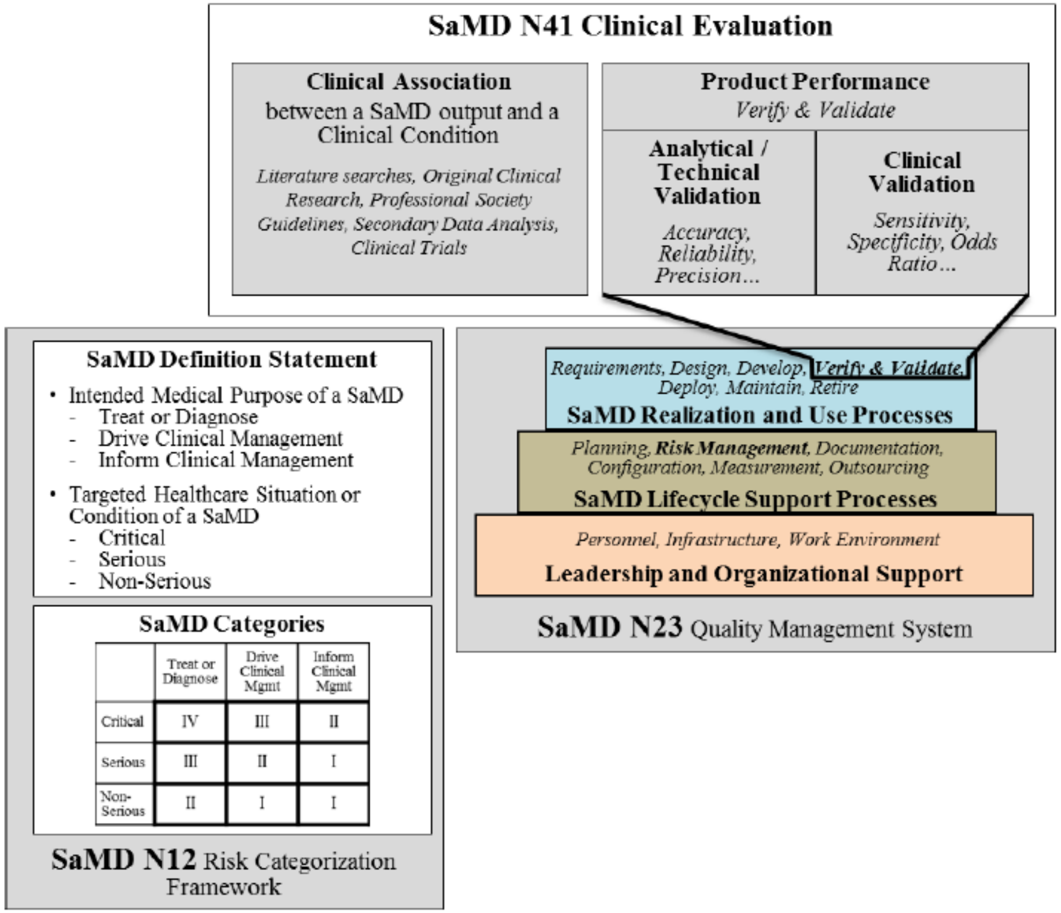


Figure 2- SaMD Landscape

Performance verification

Risk analysis

Risk

- The combination of the probability of occurrence of harm and the severity of that harm.

Patient harm

- Physical injury or damage to the health of patients, including death.

Risk Analysis

- The systematic use of available information to identify hazards and to estimate the risk.

Threat

- a process that magnifies the likelihood of a negative event, such as the exploit of a vulnerability.

Vulnerability

- a weakness in the infrastructure, networks or applications that potentially exposes to threats.

Cybersecurity risks

Process of **preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred** from a medical device to an external recipient.

DATA AND INFORMATION PROTECTION

↓

DATA PRIVACY/ CONFIDENTIALITY

PROTECTION OF SOFTWARE FUNCTIONALITY

↓

PATIENT'S SAFETY

Types od cybersecurity risks

Loss of authenticity

- the property of being genuine and being able to be verified and trusted; confidence that the contents of a message originates from the expected party and has not been modified during transmission or storage

Loss of availability

- the property of data, information, and information systems to be accessible and usable on a timely basis in the expected manner (i.e. the assurance that information will be available when needed).

Loss of integrity

- the property of data, information and software to be accurate and complete and have not been improperly modified

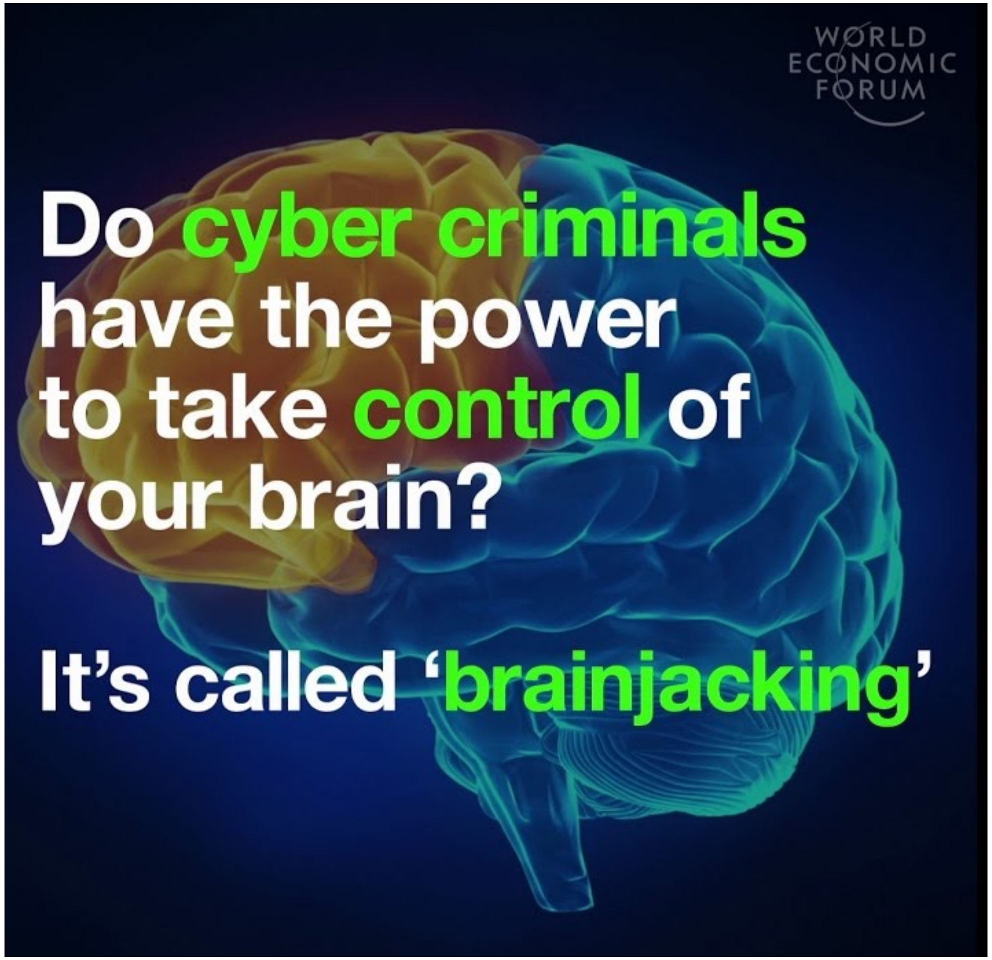
Loss of confidentiality

- the property of data, information, or system structures to be accessible only to authorized persons and entities and are processed at authorized times and in the authorized manner, thereby helping ensure data and system security. Confidentiality provides the assurance that no unauthorized users (i.e., only trusted users) have access to the data, information, or system structures.

Level of cybersecurity risk

Higher cybersecurity risk	Standard cybersecurity risk
• The device is capable of connecting (e.g., wired, wirelessly) to another medical or non-medical product, or to a network, or to the Internet; AND • A cybersecurity incident affecting the device could directly result in patient harm to multiple patients. • Examples: implantable cardioverter, defibrillators (ICDs), pacemakers, left ventricular assist devices (LVADs), brain stimulators and neurostimulators, dialysis devices, infusion and insulin pumps, and the supporting connected systems that interact with these devices such as home monitors and those with command and control functionality such as programmers.	• Medical device not meeting the criteria for higher risk

Protection of software



- Neuromodulation devices
- Pacemakers
- Implantable defibrillators

PHYSICAL SAFETY: DATA BACKUP

POSSIBLE CAUSES

- Service interrupted (heartquakes, fire, energy, malware)
- Distruction (natural events)
- Theft (or delete)

BACKUP LEVELS

- Local backup (immediate, RAID, mirror disks)
- Remote backup with short recovery time (depends on the system and the network)
- Remote backup with long recovery time (>30 km, non continuous)

Data protection: basic concepts

Authentication:

- Process of verifying the identity of an object/actor

Identification

- Autentication that defines univocally the identity of an object/actor

Authorization

- Process of allowing to use a specific object or accessing a specific information

Access control

- Process guaranteeing that the content of an object is known only to its creator or to whom is allowed to use it

Accountability

- Signature of who is responsible for the content of an object (cannot be denied)

Audit

- Process that guarantee that the security measures declared are properly set up and working

Cybersecurity core concepts: CIA

Confidentiality

- defined by the International Organization for Standardization in ISO/IEC 27002 as “ensuring that information is accessible only to those authorized to have access.”
- confidentiality breach primarily means eavesdropping on information somewhere between the source (e.g., sensor) and the receiver (e.g., personal computer, physician’s computer, hospital server) or unauthorized access to stored information

Integrity

- Aka authenticity: data is not modified or deleted without authorization.
- Integrity is violated when information is changed by a user that is not authorized to do so (directly on the devices e.g., because of a virus or on the way from information source to receiver)
- Authentication technologies help ensure that the original data is not altered or deleted during the transfer. They also provide technological means to check if the data came from the right sender and not from a sender that only pretends to be the sender (electronic signatures and certificates).

Availability

- The information is available when it is needed by authorized users.

Non repudiation

- undeniable and immutable account about where the received information originates, where it is going, who is requesting it, and who is providing it, in such a way that no entity can deny what its contribution was to the overall activity.
- Non-repudiation can be achieved through electronic signatures and audit trails.

Ensuring data protection: cybersecurity measures

Prevent all unauthorized use

Ensure code, data, and execution integrity

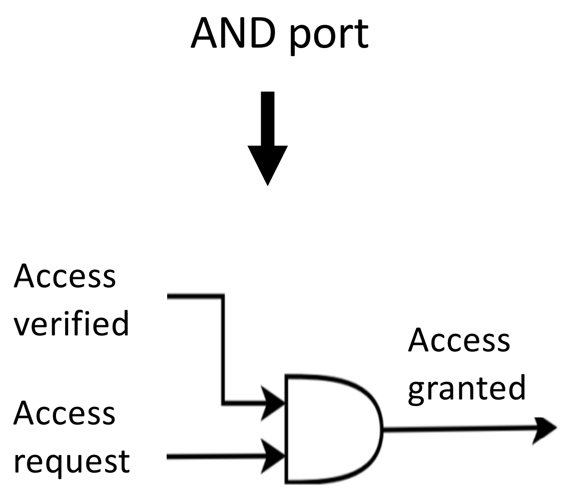
Protect confidentiality of data

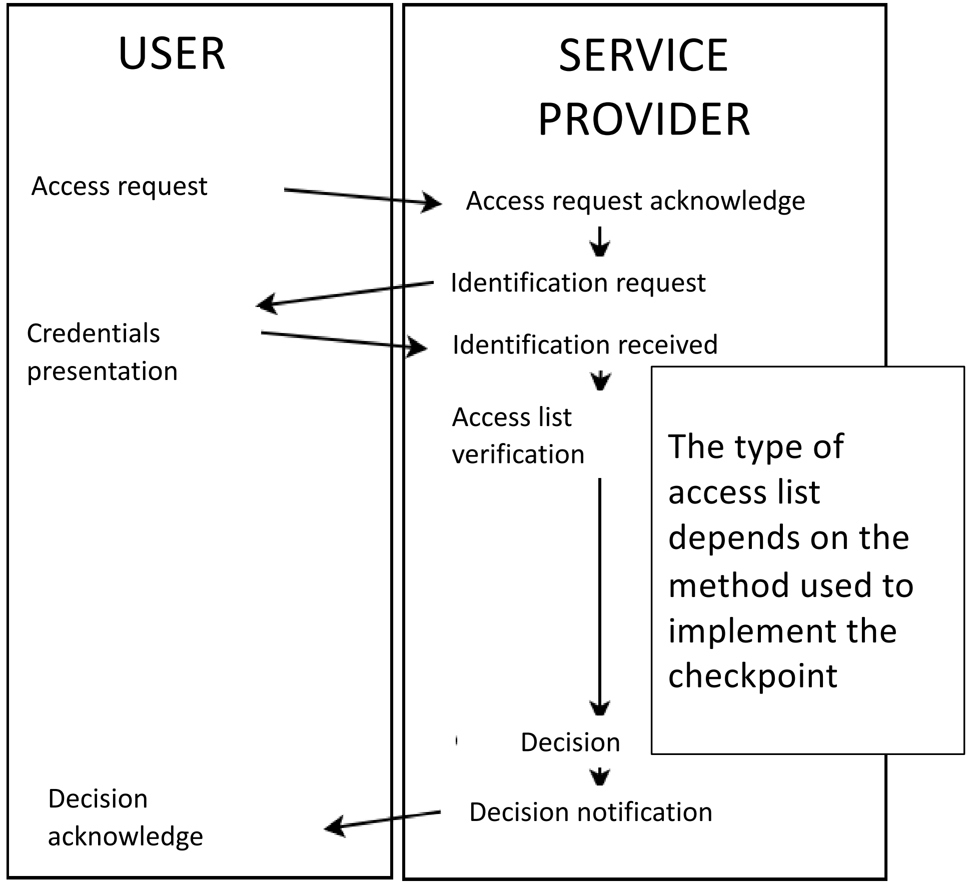
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
Draft Guidance for Industry and Food and Drug Administration Staff
October 2018

Prevent unauthorized use: Access to trusted users and devices

- Limit access to devices through the **authentication of users**
- Use automatic timed methods to terminate sessions within the system where appropriate for the use environment.
- Employ a **layered authorization model** by differentiating privileges based on the user role (e.g., caregiver, patient, health care provider, system administrator) or device functions.
- Use appropriate authentication (e.g., multi-factor authentication to permit privileged device access to system administrators, service technicians, maintenance personnel).
- Strengthen password protection. Do not use credentials that are hardcoded, default, easily-guessed, easily compromised (i.e., passwords which are the same for each device; unchangeable; can persist as default; difficult to change; and vulnerable to public disclosure). Limit public access to passwords used for privileged device access.
- Consider **physical locks on devices** and their communication ports to minimize tampering.

AUTHENTICATION AND IDENTIFICATION





METHODS OF AUTHENTICATION

AUTHENTICATION METHODS

CIÒ CHE SI SA (informazione)

Informazioni che solo il soggetto può conoscere

Password, passphrase, PIN, codice di accesso

Facilità di individuazione/difficolta di memorizzazione

CIÒ CHE SI HA (oggetti)

Basati su qualcosa che l'individuo possiede: Smart card, badge,

Custodia del dispositivo/facilità di smarrimento

Necessità di punti lettori

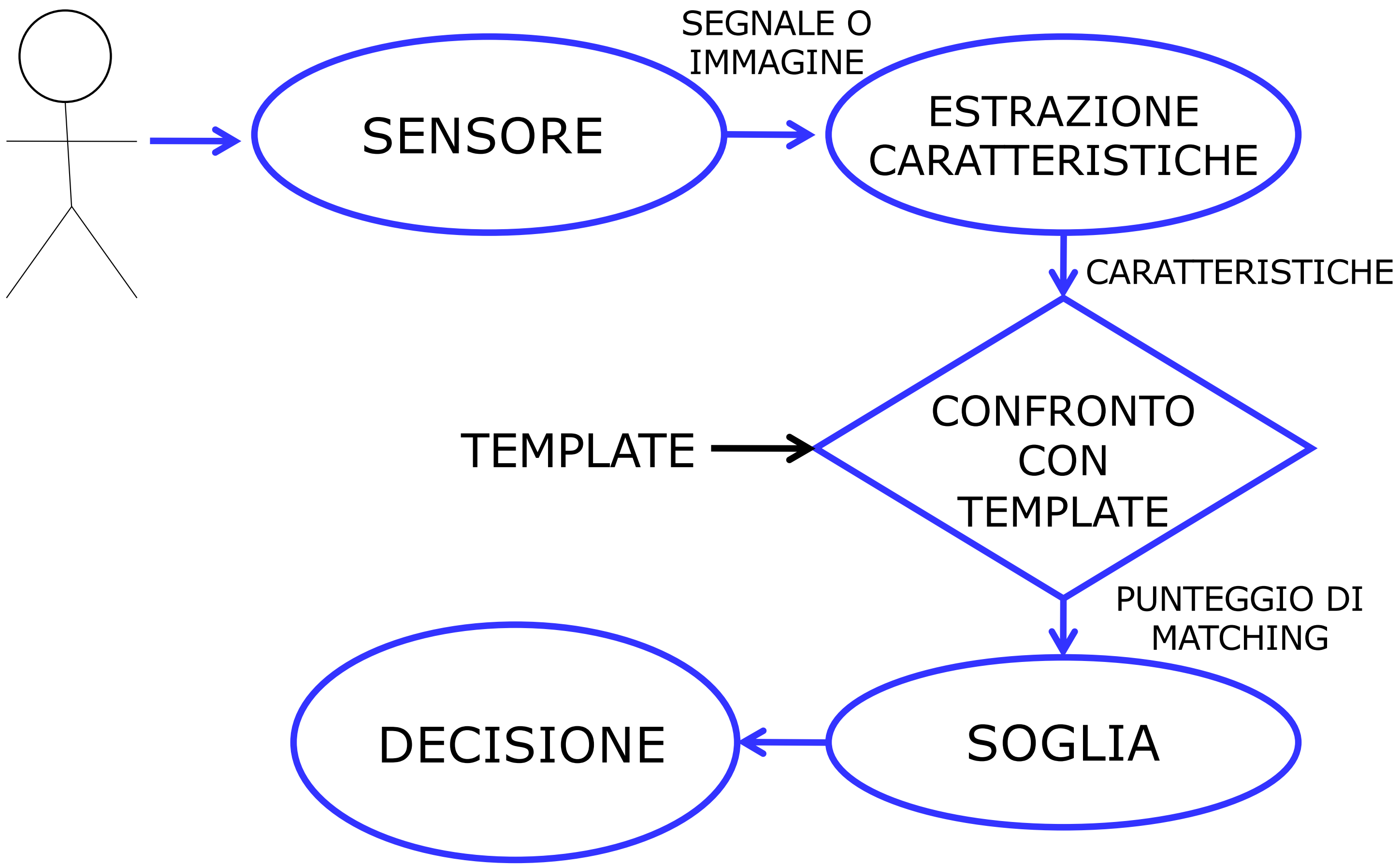
CIÒ CHE SI È (caratteristiche personali)

Riconoscimento biometrico=valutazione delle caratteristiche fisiche o comportamentali del soggetto

Non possono essere segreti

Identificazione non certa

BIOMETRIA



SENSORE
SEGNALE O IMMAGINE
ESTRAZIONE CARATTERISTICHE
CARATTERISTICHE
TEMPLATE
CONFRONTO CON TEMPLATE
PUNTEGGIO DI MATCHING
SOGLIA
DECISIONE

EFFETTO DELLA SOGLIA

- L'identificazione basata su biometria non è certa perchè è basata su caratteristiche personali che non sono sempre stabili
- Elementi di variabilità:
  - Variabilità intrinseca della caratteristica biometrica (es: voce rauca, mano sudata, etc.)
  - Variabilità introdotta dal sensore (es: sensore sporco)
  - Variabilità del metodo di misurazione (es: posizione dell'occhio rispetto al sensore)
  - Fattori esterni (es: luminosità dell'ambiente, rumore di fondo)
  - Incertezza della stima della caratteristica (metodo matematico di stima o ricostruzione)
- Esiste una probabilità di errore calcolabile utilizzando misure di accuratezza

MISURE DI ACCURATEZZA

- Matrice di confusione (in epidemiologia)

		REALE	
		POSITIVO	NEGATIVO
PREDETTO/ STIMATO	POSITIVO	VERI POSITIVI	FALSI POSITIVI
	NEGATIVO	FALSI NEGATIVI	VERI NEGATIVI

TOTALE = VP+FN+FP+VN
ACCURATEZZA = (VP+VN)/TOTALE
SENSIBILITÀ = VP/(VP+FN) – proporzione di valori riconosciuti come positivi tra tutti i positivi
SPECIFICITÀ = VN/(FP+VN) – proporzione dei valori riconosciuti come negativi tra tutti i negativi

FAILURE TO ENROLL

Nei sistemi biometrici si valuta anche quante volte il sistema non riesce ad acquisire il campione con qualità sufficiente per poter procedere all'identificazione.

$$FAILUREtoENROLL = \frac{num \quad arruolamenti \quad rifiutati}{totale \quad campioni}$$

DEFINITION OF USER ROLES

Current Users

System Id	Username	Given	Family Name	Roles
5-9	doctor	Jake	Smith	Organizational: Doctor
4-2	nurse	Jane	Smith	Organizational: Nurse
3-4	clerk	John	Smith	Organizational: Registration Clerk
6-7	sysadmin	Julie	Smith	Organizational: System Administrator

OpenMRS

Administration

Users

- Manage Users
- Manage Roles
- Manage Privileges
- Manage Alerts

Admin | Manage Users | Manage Roles | Manage Privileges | Manage Alerts

Add/Edit User

Demographic Info

Given * Jane

Middle

Family Name * Smith

Gender* Male Female

Provider Account

Provider Identifier(s): nurse

Login Info

System Id 4-2

Username nurse *User can log in with either Username or Sys*

User's Password* *Password should be 8 characters long and*

Confirm Password* *Retype the password (for accuracy)*

Force Password Change *Optionally require that this user change their password on next lo*

Roles

- Anonymous
- Application: Administers System
- Application: Configures Appointment Scheduling
- Application: Configures Forms
- Application: Configures Metadata
- Application: Edits Existing Encounters
- Application: Enters ADT Events
- Application: Enters Vitals
- Application: Has Super User Privileges

DEFINITION OF USER ROLES

Role* Organizational: Nurse

Description Nurse

Inherited Roles

Organizational: Nurse inherits privileges from these roles

- Application: Administers System
- Application: Configures Appointment Scheduling
- Application: Configures Forms
- Application: Configures Metadata
- Application: Edits Existing Encounters
- Application: Enters ADT Events
- Application: Enters Vitals
- Application: Has Super User Privileges
- Application: Manages Atlas
- Application: Manages Provider Schedules
- Application: Records Allergies
- Application: Registers Patients
- Application: Requests Appointments
- Application: Schedules And Overbooks Appointments
- Application: Schedules Appointments
- Application: Sees Appointment Schedule
- Application: Uses Capture Vitals App
- Application: Uses Patient Summary
- Application: Writes Clinical Notes
- Organizational: Doctor
- Organizational: Hospital Administrator
- Organizational: Registration Clerk
- Organizational: System Administrator
- Privilege Level: Full
- Privilege Level: High
- Provider
- System Developer

Privileges

Greyed out checkboxes represent privileges inherited from other role

Select/Unselect All

- Add Allergies
- Add Cohorts
- Add Concept Proposals
- Add Encounters
- Add HL7 Inbound Archive
- Add HL7 Inbound Exception
- Add HL7 Inbound Queue
- Add HL7 Source
- Add Observations
- Add Orders
- Add Patient Identifiers
- Add Patient Programs
- Add Patients
- Add People
- Add Problems
- Add Relationships
- Add Report Objects
- Add Reports
- Add Users
- Add Visits
- App: adminui.configuremetadata
- App: appointmentschedulingui.appointme
- App: appointmentschedulingui.home
- App: appointmentschedulingui.providerSc
- App: appointmentschedulingui.view
- App: atlas.manage
- App: attachments.attachments.page
- App: coreapps.activeVisits
- App: coreapps.configuremetadata
- App: coreapps.dataManagement
- App: coreapps.findPatient
- App: coreapps.mergePatient
- App: coreapps.patientDashboard
- App: coreapps.patientVisits
- App: coreapps.summaryDashboard
- App: coreapps.systemAdministration
- App: formentryapp.forms

Prevent unauthorized use: authenticate and check authorization of safety-critical commands

- Use **authentication to prevent unauthorized access to device functions** and to prevent unauthorized (arbitrary) software execution.
- Require **user authentication before permitting software or firmware updates**, including those affecting the operating system, applications, and anti-malware.
- Use **cryptographically strong authentication** resident on the device to authenticate personnel, messages, commands and as applicable, all other communication pathways
- **Authenticate all external connections**. For example, if a device connects to an offsite server, then it and the server should mutually authenticate, even if the connection is initiated over one or more existing trusted channels.
- **Authenticate firmware and software**. Verify authentication tags (e.g., signatures, message authentication codes (MACs)) of software/firmware content, version numbers, and other metadata. The version numbers intended to be installed should themselves be signed /haveMACs. Devices should be electronically identifiable (e.g.,model number, serial number) to authorized users.
- **Perform authorization checks** based on authentication credentials or other irrefutable evidence. For example, a medical device programmer should have elevated privileges that are granted based on cryptographic authentication or a signal of intent that cannot physically be produced by another device, e.g., a home monitor, with a software-based attack.
- Devices should be designed to **"deny by default,"** i.e., that which is not expressly permitted by a device is denied by default. For example, the device should generally reject all unauthorized connections (e.g., incoming TCP, USB, Bluetooth, serial connections).
- The **principle of least privilege** should be applied to allow only the level of access necessary to perform a function.

Criptography

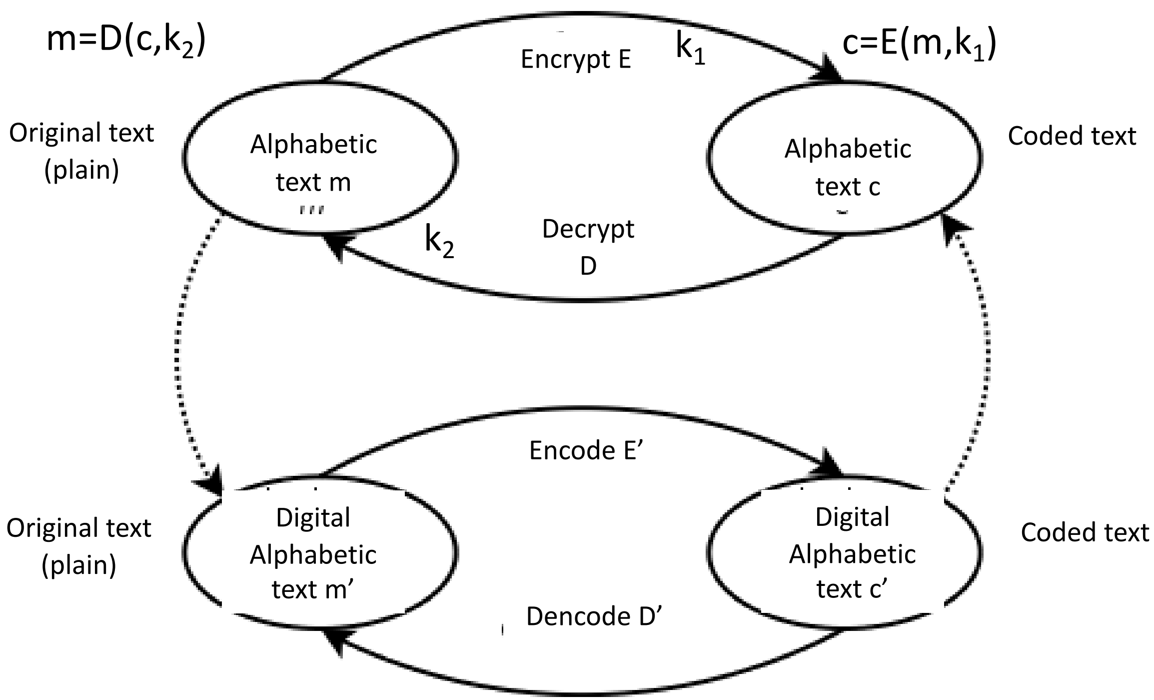
CRYPTOGRAPHY is the practice and study of techniques for **secure communication** in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that prevent adversaries to understand the content of the message

The word cryptography comes from the Greek words *kryptos* meaning hidden and *graphein* meaning writing

CRYPTOGRAPHY ARCHITECTURE

ALGORITHM → Mathematical process or method that transforms a plain text into a non-readable text

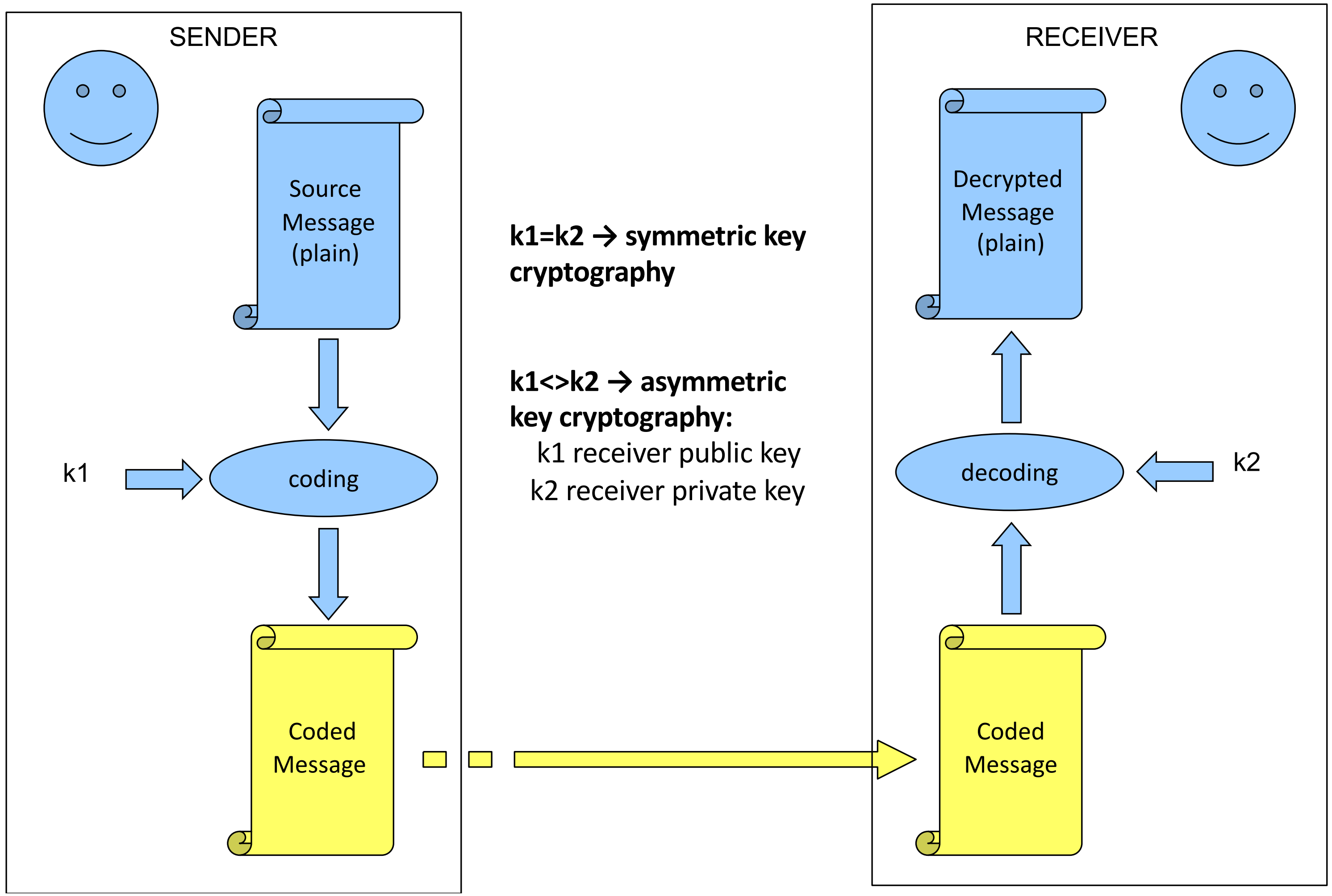
KEY (k_i) → Information (usually alphanumeric) that is able to modify te behaviour of the cryptographyc algorithm.



KERCHKHOFFS PRINCIPLE

- The security of a cryptosystem should depend solely on the secrecy of the key and the private randomizer.
- A method of secretly coding and transmitting information should be secure even if everyone knows how it works

SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY



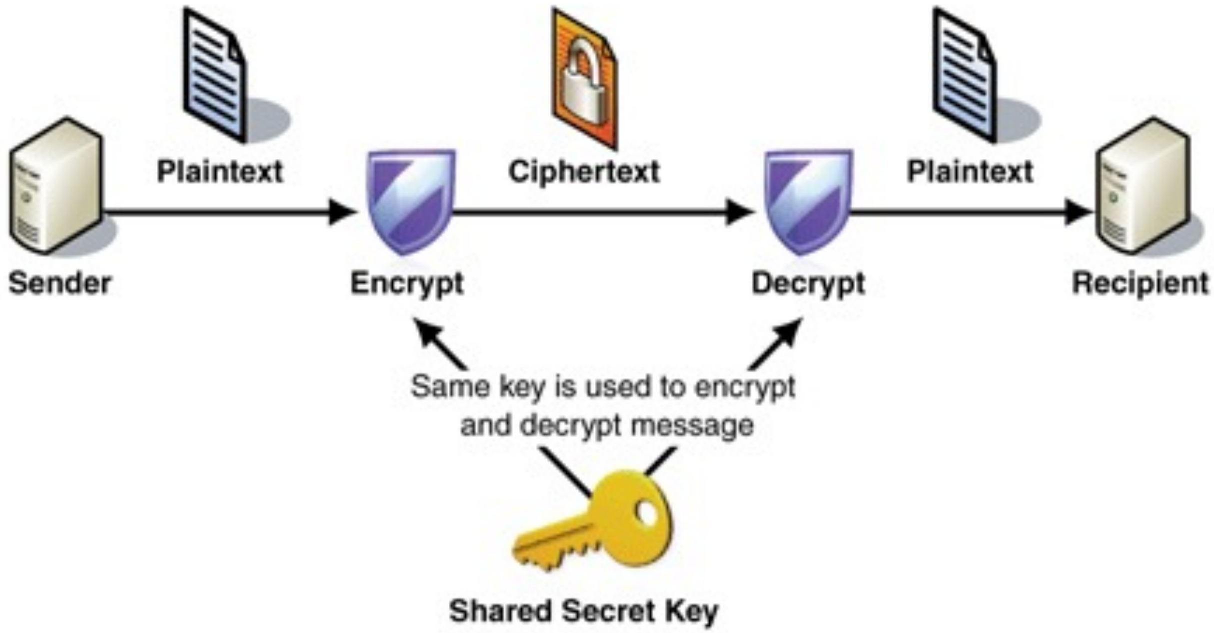
k1=k2 → symmetric key cryptography

k1<>k2 → asymmetric key cryptography:

k1 receiver public key

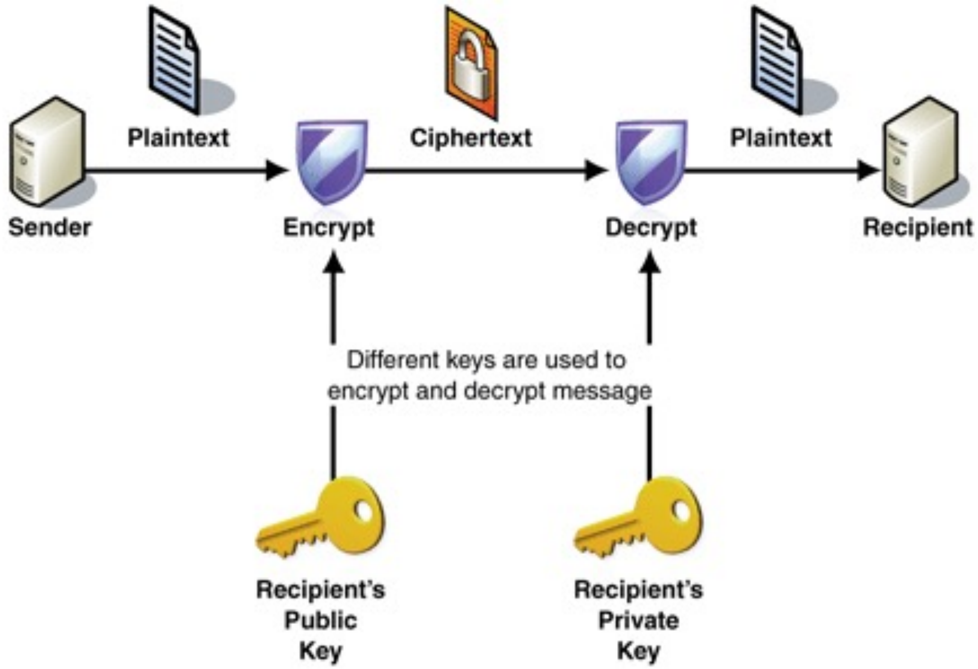
k2 receiver private key

SYMMETRIC ENCRYPTION



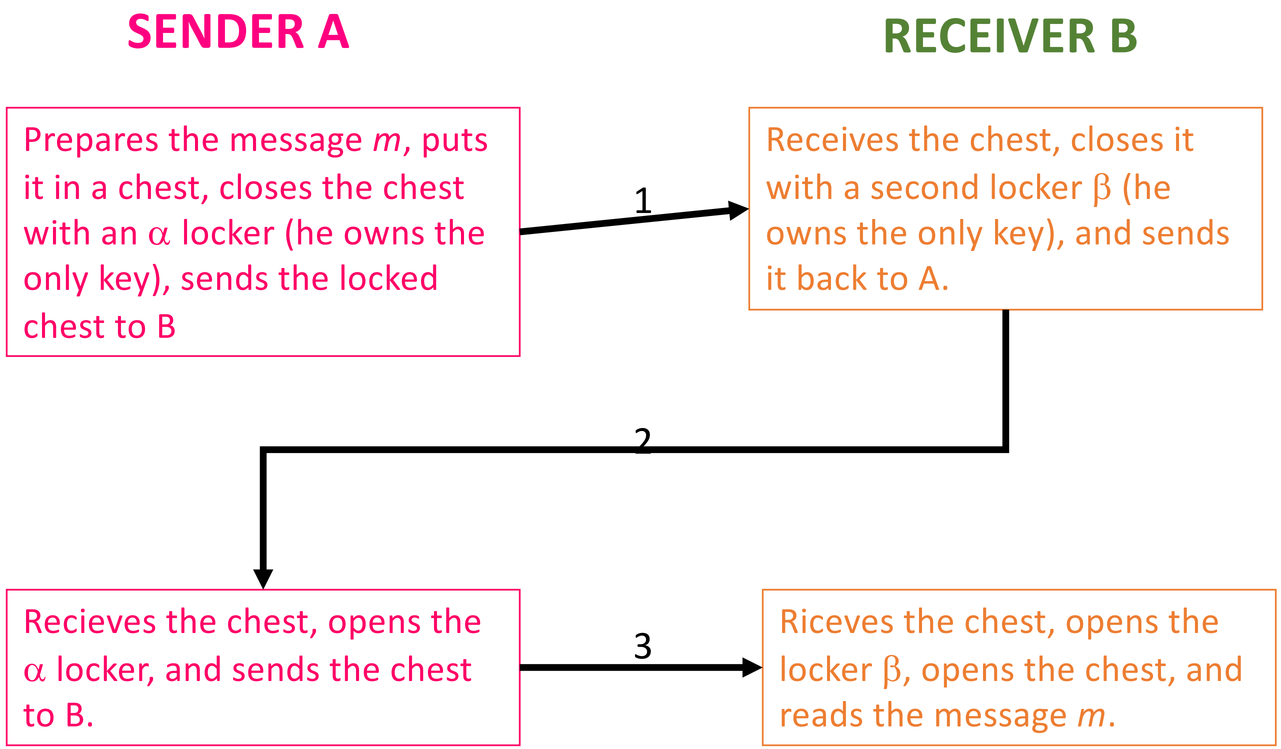
- The sender and the recipient have to share the key
- The key is used both to encrypt and to decrypt

ASYMMETRIC ENCRYPTION



- The public key of the recipient is used only to encrypt data (cannot decrypt). It can be openly distributed to those who want to encrypt a message to the recipient.
- The private key of the recipient is used to decrypt messages, and only the recipient must be able to access it.

ASYMMETRIC ALGORITHMS: THE TWO LOCKERS MECHANISM



SYMMETRIC VS ASYMMETRIC CRYPTOGRAPHY

	Advantages	**Disvantages**
Symmetric key	▪Easy to implement ▪Low computational requirements → speed execution	▪Need to share the key
Asymmetric key	▪Different keys for the sender and the receiver ▪Knowing the public key does not allow decrypting the message	▪More difficult to implements ▪High computational requirements → slow execution

Secure Socket Layer (SSL)

- The Secure Sockets Layer (SSL) is a computer networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients.
- SSL uses a combination of public-key and symmetric-key encryption to secure a connection between two machines, typically a Web or mail server and a client machine, communicating over the Internet or an internal network.

How SSL works

- The SSL protocol includes two sub-protocols: the record protocol and the "handshake" protocol.
- These protocols allow a client to authenticate a server and establish an encrypted SSL connection: a server that supports SSL presents its digital certificate to the client to authenticate the server's identity.
- The authentication process uses public-key encryption to validate the digital certificate and confirm that a server is in fact the server it claims to be.
- Once the server has been authenticated, the client and server establish cipher settings and a shared key to encrypt the information they exchange during the remainder of the session.
- The handshake also allows the client to authenticate itself to the server. In this case, after server authentication is successfully completed, the client must present its certificate to the server to authenticate the client's identity before the encrypted SSL session can be established.

Ensure trusted content: code integrity

- Only **allow installation of cryptographically verified firmware/software updates**. Use cryptographically signed updates to help prevent unauthorized reduction in the level of protection (downgrade or rollback attacks) by ensuring that the new update is more recent than the currently installed version.
- Where feasible, ensure that **the integrity of software is validated prior to execution**, e.g., ‘whitelisting’ based on digital signatures.

Ensure trusted content: data integrity

- Verify the integrity of all incoming data (ensuring it is not modified in transit or at rest, and it is well-formed/compliant with the expected protocol/specification).
- Ensure capability of secure data transfer to and from the device, and when appropriate, use methods for encryption and authentication of the end points with which data is being transferred.
- Protect the integrity of data necessary to ensure the safety and essential performance of the device.
- Use current recommended standards for cryptography and for cryptographic protection for communications channels.
- Use unique per device cryptographically secure communication keys to prevent leveraging the knowledge of one key to access a multitude of devices.

Ensuring data integrity: digest

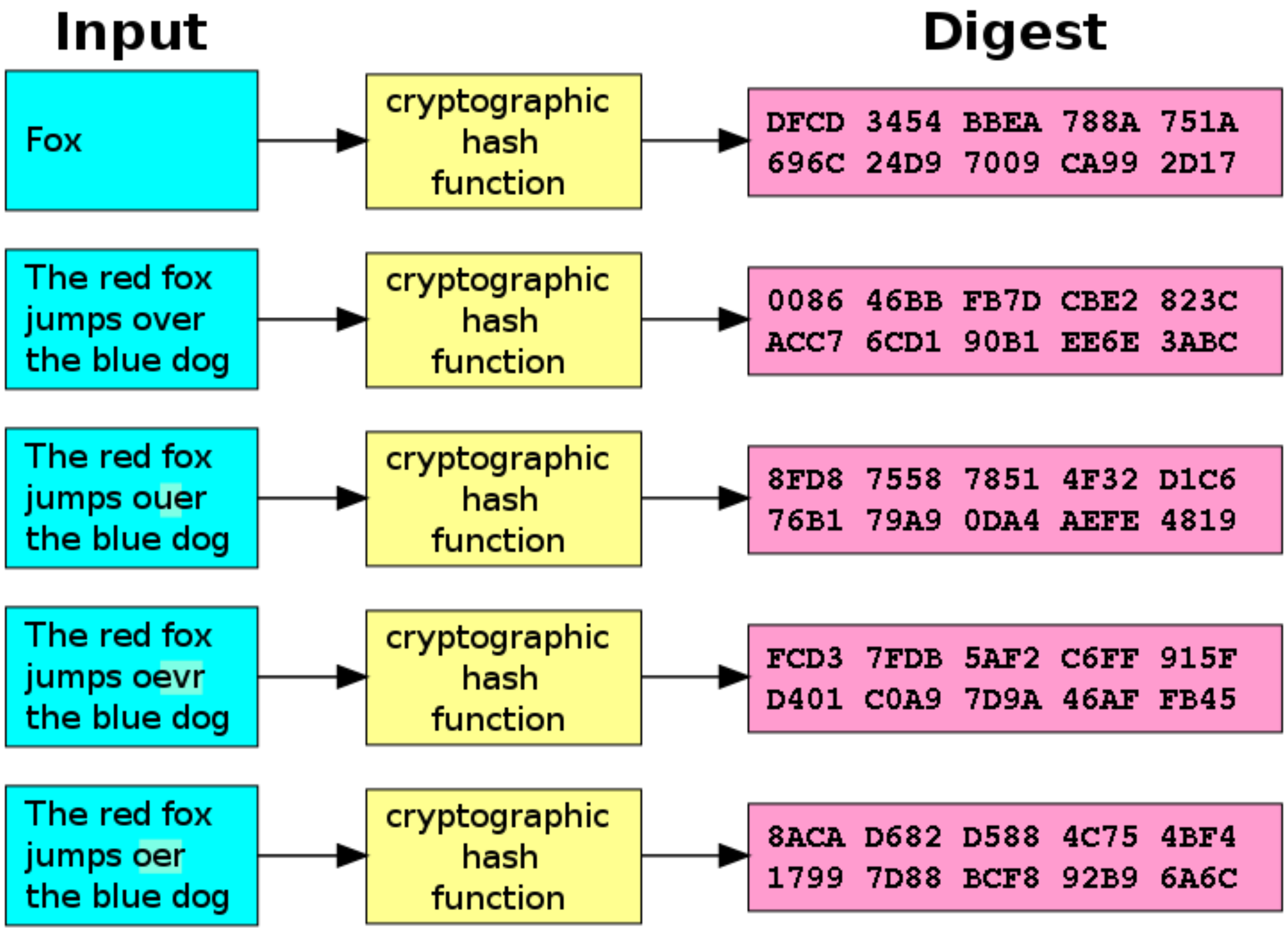
- To ensure document integrity it is possible to use HASH FUNCTIONS (implementing message DIGEST):
- **DIGEST →**
  - Short string of predefined length
  - Characterizes the document
  - Verify the integrity of the document itself
  - Calculated by the sender, sent to the receiver, calculated by the receiver and compared to the one that the receiver received → if the two match → the integrity of the document is preserved

HASH FUNCTIONS

- Message/Document digests are created through hash functions

- The ideal hash function **has four main properties**:
  - it is **easy to compute** the hash value for any given message
  - it is **infeasible to generate a message from its hash**
  - it is **infeasible to modify a message without changing the hash**
  - it is **infeasible to find two different messages with the same hash**.

MESSAGE DIGEST EXAMPLE



Ensure trusted content: execution integrity

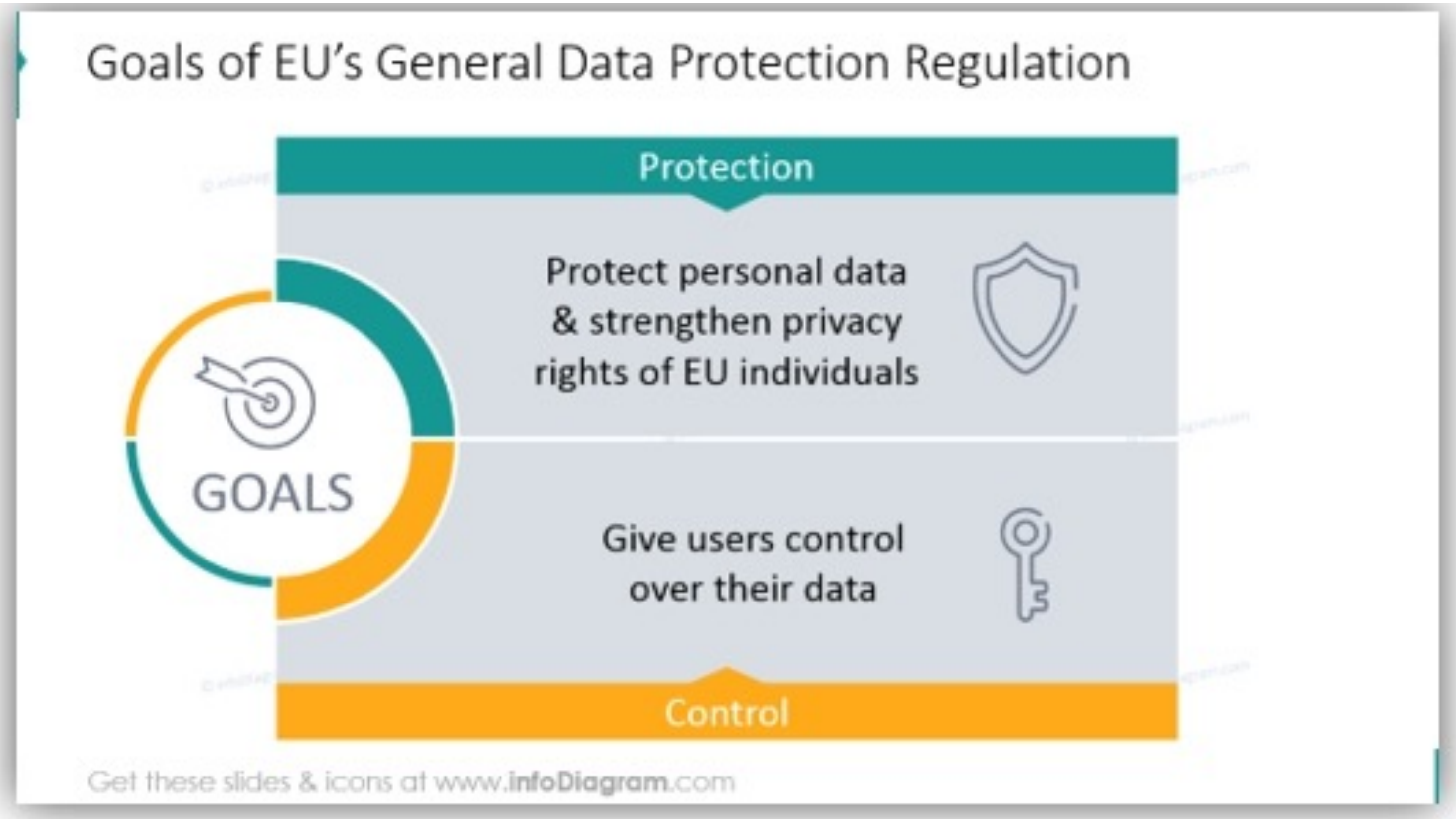
- Where feasible, use industry-accepted best practices to maintain/verify integrity of code while it is being executed on the device.

Privacy and confidentiality

- Privacy is an important part of confidentiality, especially when it comes to protected health information(PHI).
- PHI is defined as individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium (45CFR160.103 [B1]).
- The U.S. Health Insurance Portability and Accountability Act (HIPAA) limits the circumstances in which an individual's PHI may be used or disclosed by covered entities (HHS [B7]).
- Similarly, the EU General Data Protection Regulation states that personal data shall be processed lawfully, fairly, and in a transparent manner; collected for specified, explicit, and legitimate purpose; and kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (Official Journal of the EU [B19]).
- loss of confidential protected health information (PHI), are not considered "patient harms" but are regulated by national privacy rules (GDPR, HIPAA)

Protection of data

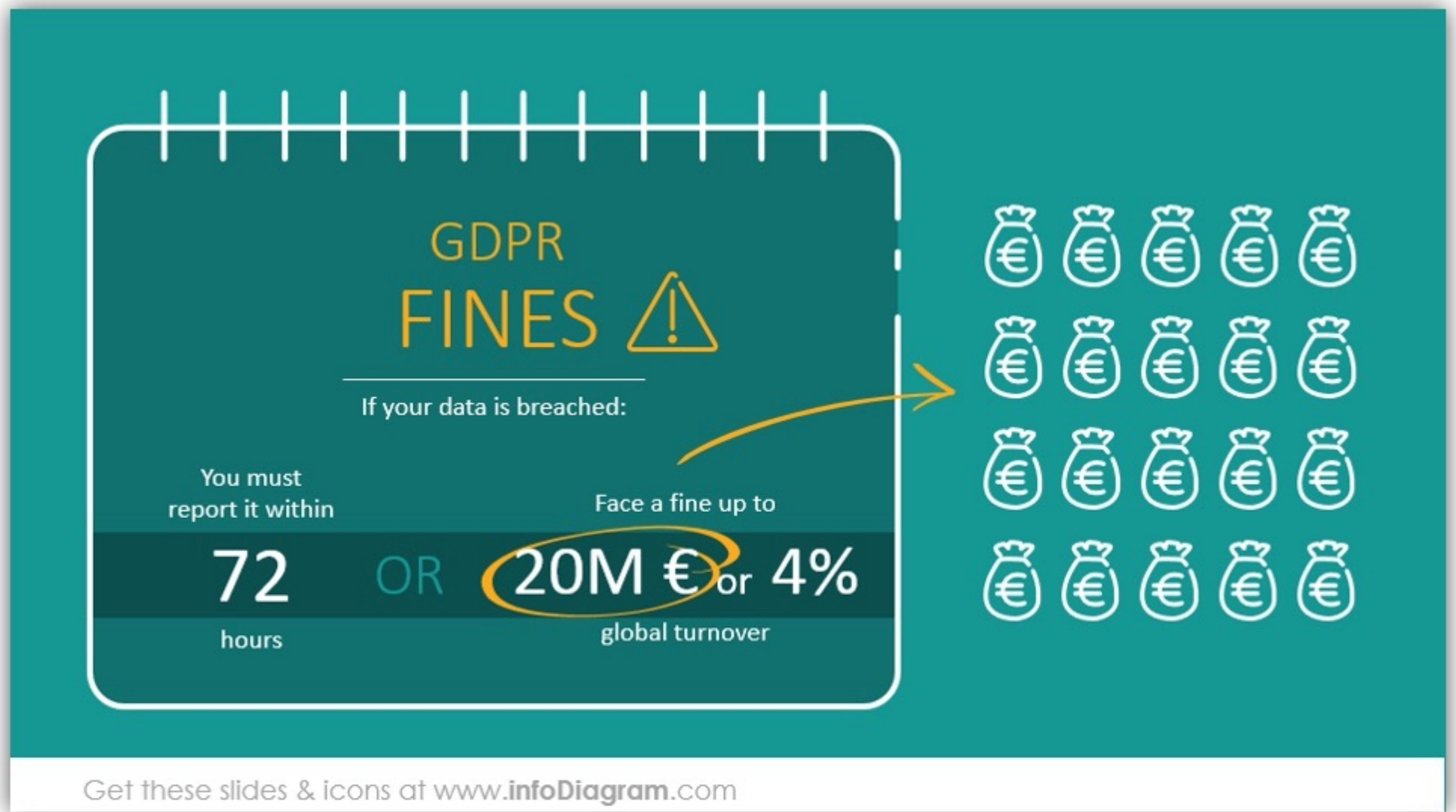
GDPR: GOALS


Goals of EU's General Data Protection Regulation
Protection
Protect personal data & strengthen privacy rights of EU individuals
GOALS
Give users control over their data
Control
Get these slides & icons at www.infoDiagram.com

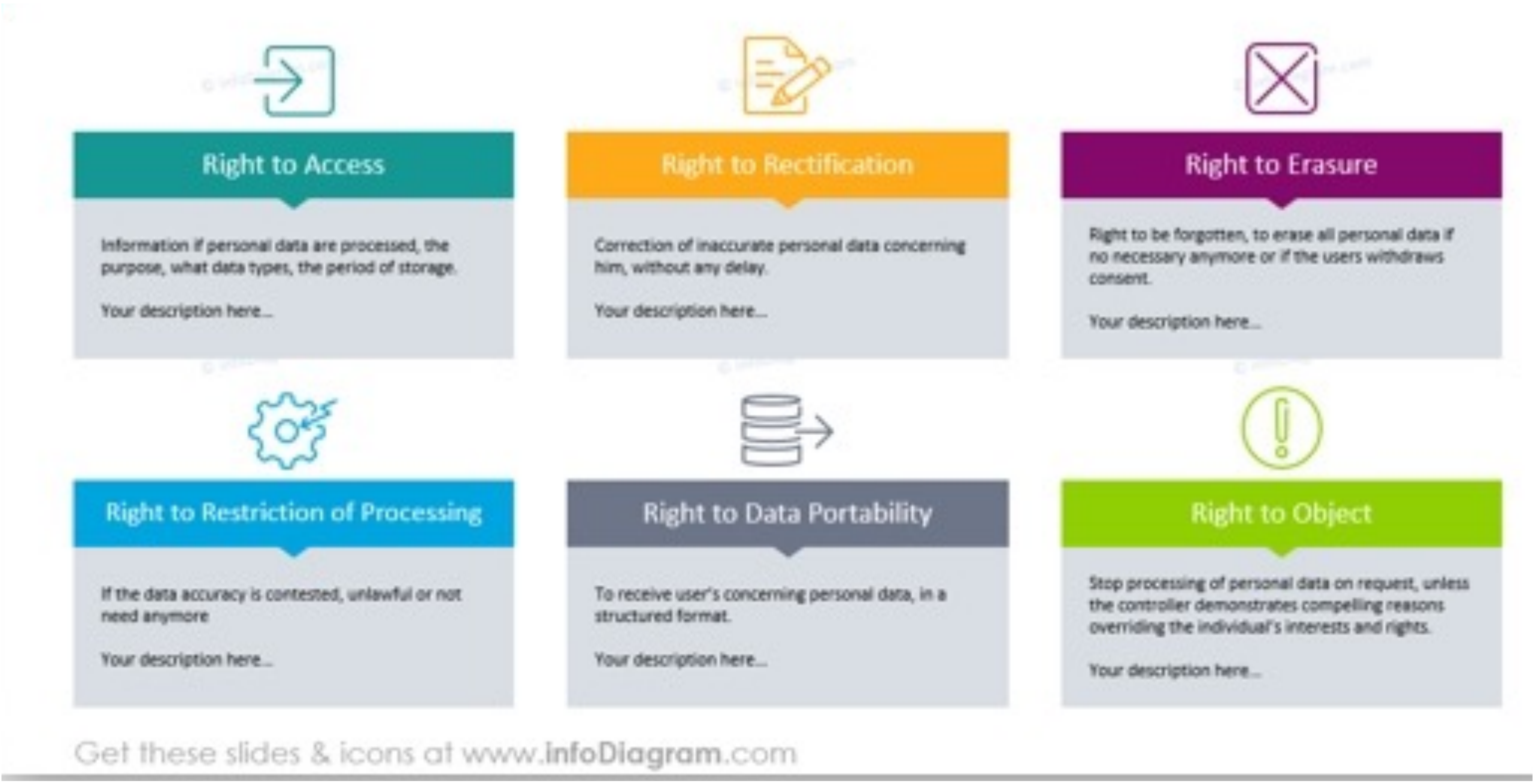
GDPR: PERSONAL DATA AND PROCESSING

Processing: operations performed on personal data, including by manual or automated means. It includes the **collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination** or otherwise making available, **alignment or combination, restriction, erasure or destruction** of personal data.

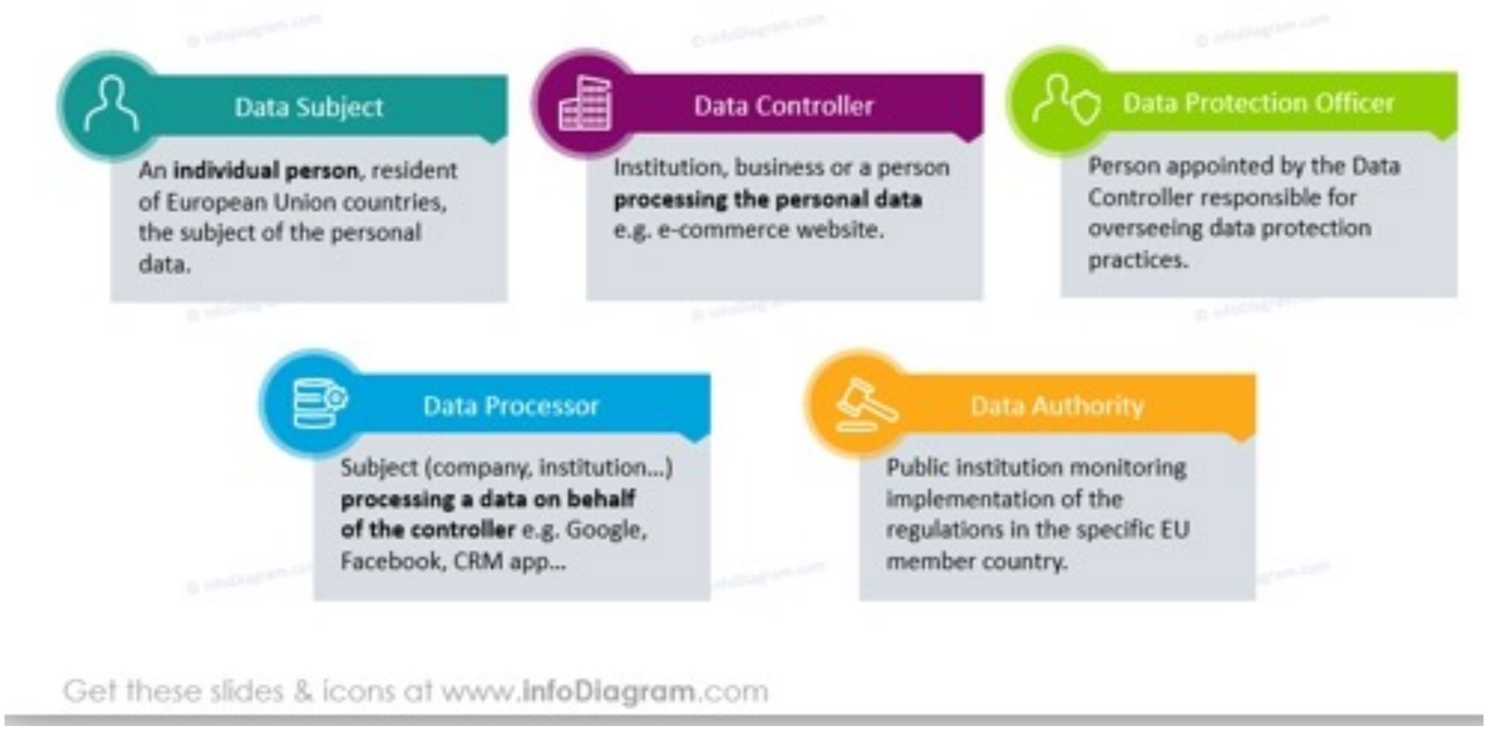
GDPR: FINES


GDPR
FINES
If your data is breached:
You must
report it within
72
hours
OR
Face a fine up to
20M € or 4%
global turnover
Get these slides & icons at www.infoDiagram.com

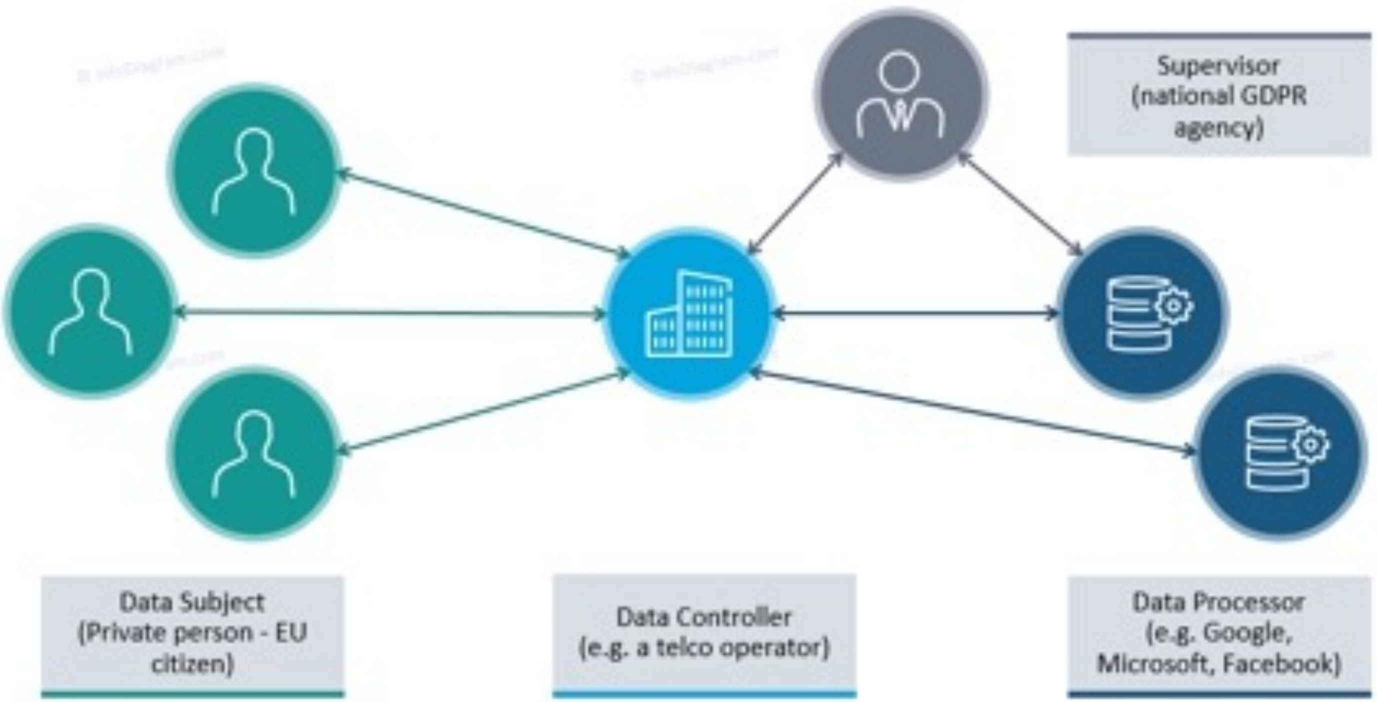
GDPR: INDIVIDUAL RIGHTS



GDPR SUBJECTS



GDPR SUBJECTS



HIPAA security rule

- The HIPAA Security Rule contains the standards that must be applied in order to safeguard and protect electronically created, accessed, processed, or stored PHI (ePHI) when at rest and in transit.
- It has three parts:
  - technical safeguards
  - physical safeguards
  - administrative safeguards

HIPAA technical safeguard

Implementation Specification	Required or Addressable	Further Information
Implement a means of access control	Required	This not only means assigning a centrally-controlled unique username and PIN code for each user, but also establishing procedures to govern the release or disclosure of ePHI during an emergency.
Introduce a mechanism to authenticate ePHI	Addressable	This mechanism is essential in order to comply with HIPAA regulations as it confirms whether ePHI has been altered or destroyed in an unauthorized manner.
Implement tools for encryption and decryption	Addressable	This guideline relates to the devices used by authorized users, which must have the functionality to encrypt messages when they are sent beyond an internal firewalled server, and decrypt those messages when they are received.
Introduce activity logs and audit controls	Required	The audit controls required under the technical safeguards are there to register attempted access to ePHI and record what is done with that data once it has been accessed.
Facilitate automatic log-off of PCs and devices	Addressable	This function logs authorized personnel off of the device they are using to access or communicate ePHI after a pre-defined period of time. This prevents unauthorized access of ePHI should the device be left unattended.

HIPAA physical safeguard

Implementation Specification	Required or Addressable	Further Information
Facility access controls must be implemented	Addressable	Controls who has physical access to the location where ePHI is stored and includes software engineers, cleaners, etc. The procedures must also include safeguards to prevent unauthorized physical access, tampering, and theft.
Policies for the use/positioning of workstations	Required	Policies must be devised and implemented to restrict the use of workstations that have access to ePHI, to specify the protective surrounding of a workstation and govern how functions are to be performed on the workstations.
Policies and procedures for mobile devices	Required	If users are allowed to access ePHI from their mobile devices, policies must be devised and implemented to govern how ePHI is removed from the devices if the user leaves the organization or the device is re-used, sold, etc.
Inventory of hardware	Addressable	An inventory of all hardware must be maintained, together with a record of the movements of each item. A retrievable exact copy of ePHI must be made before any equipment is moved.

HIPAA administrative safeguard

Implementation Specification	Required or Addressable	Further Information
Conducting risk assessments	Required	Among the Security Officer´s main tasks is the compilation of a risk assessment to identify every area in which ePHI is being used, and to determine all of the ways in which breaches of ePHI could occur.
Introducing a risk management policy	Required	The risk assessment must be repeated at regular intervals with measures introduced to reduce the risks to an appropriate level. A sanctions policy for employees who fail to comply with HIPAA regulations must also be introduced.
Training employees to be secure	Addressable	Training schedules must be introduced to raise awareness of the policies and procedures governing access to ePHI and how to identify malicious software attacks and malware. All training must be documented.
Developing a contingency plan	Required	In the event of an emergency, a contingency plan must be ready to enable the continuation of critical business processes while protecting the integrity of ePHI while an organization operates in emergency mode.
Testing of contingency plan	Addressable	The contingency plan must be tested periodically to assess the relative criticality of specific applications. There must also be accessible backups of ePHI and procedures to restore lost data in the event of an emergency.
Restricting third-party access	Required	It is vital to ensure ePHI is not accessed by unauthorized parent organizations and subcontractors, and that Business Associate Agreements are signed with business partners who will have access to ePHI.
Reporting security incidents	Addressable	The reporting of security incidents is different from the Breach Notification Rule (below) inasmuch as incidents can be contained and data retrieved before the incident develops into a breach.

Secure by design and secure by default

Secure by design means that the software has been designed from the ground up to be secure. Under Secure by Design principles, manufacturers may assume the existence of malicious activities and take care to minimize the impact when an attempt is made to exploit a system.

Secure by default is the concept of designing the system so that it operates by default with a minimal required set of functionalities with a secure configuration.

Secure by design and secure by default include, but are not limited to, the following:

— **Least privileges:** All components and users operate with the fewest possible permissions.
— **Defense in depth:** Design does not rely on a single threat mitigation solution alone for protection; rather, layers of protection are implemented.
— **Secure default settings:** Based on the known attack surfaces for the system, the design minimizes the attack surfaces in the default configuration.
— **Avoidance of insecure operating system changes:** Applications do not make or require any default changes to the operating system or security settings that reduce security for the host computer without consideration of possible risks.
— **Services off by default:** The services off by default allows that, if a feature of a system is rarely used, that feature is deactivated by default.

Privacy by design and privacy by default

Privacy by design means that privacy and data protection are embedded throughout the entire system lifecycle, from the early design stage to deployment, use, and ultimate disposal. This concept includes, but is not limited to, the following:

— **Provide notice of privacy practices to users:** Provide appropriate notice to users about data that is collected, stored, or shared so that users can make informed decisions about how their personal information is used and disclosed.

— **Do not store secrets:** Collect the minimum amount of data that is required for a particular purpose and use the least sensitive form of that data.

— **Protect secrets and secret data; de-identification:** Encrypt sensitive data at rest and in transfer, limit access to stored data, and verify that data usage complies with the system's intended use. If encryption is not possible, anonymize patient data (e.g., log and trace files).

Privacy by default means that privacy and data protection are embedded as default configuration settings in a system. This concept includes, but is not limited to, the following:

— **Least privileges:** Ship with secure default privacy settings, and prevent unauthorized access through technical controls.

— **Do not store secrets:** Process and store only minimum necessary data. Retain data for the shortest possible time.

— **Protect secrets and secret data:** Protect any sensitive data at rest and in transit with access controls and encryption.

Cybersecurity measures: detect, respond, and recover

- Appropriate design should anticipate the need to detect and respond to dynamic cybersecurity risks, including the need for deployment of cybersecurity routine updates and patches as well as emergency workarounds
- Detect:
  - Routine security and antivirus scanning
  - Tracking and control of software updates
- Respond:
  - User notification of cybersecurity risk detection
  - Architecture to rapid deploy of patches and updates
- Recover:
  - Implement features to protect critical functionality
  - Recovery of device configuration by authorized user

Approach to cybersecurity assessment

IEEE Std 11073-40101™-2020

Health informatics—Device interoperability

Part 40101:
Foundational—Cybersecurity—
Processes for vulnerability assessment

Developed by the

IEEE 11073 Standards Committee
of the
IEEE Engineering in Medicine and Biology Society

Approved 24 September 2020

IEEE SA Standards Board

IEEE Std 11073-40102™-2020

Health informatics—Device interoperability

Part 40102:
Foundational—Cybersecurity—
Capabilities for mitigation

Developed by the

IEEE 11073 Standards Committee
of the
IEEE Engineering in Medicine and Biology Society

Approved 24 September 2020

Family of standards devoted to point-of-care/personal complex eHealth devices/systems requiring interoperability

Cybersecurity risk management

Identification of assets, threats, and vulnerabilities

↓

Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;

↓

Assessment of the likelihood of a threat and of a vulnerability being exploited

↓

Determination of risk levels and suitable mitigation strategies;

↓

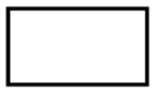
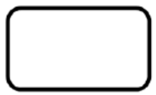
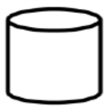
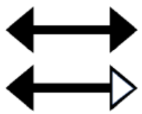
Assessment of residual risk and risk acceptance criteria

Identification of threats step 1: system modeling

- Formal process and system modeling helps identifying threats and vulnerabilities
- Multiple techniques:
  - UML
  - Data flow diagrams (DFDs)

Data Flow Diagrams

DFDs are a way to represent the entities involved with the functioning of the medical device, how those entities are related, and the assumed trust boundaries between them.

Element	Symbol	Discussion
External Entity		**Object:** A sharp-cornered rectangle. **Represents:** Anything outside your control. Examples include people and systems run by other organizations or even divisions.
Process		**Object:** A rounded rectangle. **Represents:** Any running code, including compiled, scripts, shell commands, Structured Query Language (SQL) stored procedures, et cetera.
Data Store		**Object:** A drum. **Represents:** Anywhere data is stored, including files, databases, shared memory, cloud storage services, cookies, et cetera.
Data Flows		**Object:** A double-headed arrow. **Represents:** All the ways that processes can talk to data stores or each other. If a conversation is only initiated by one side, you can represent the initiating side as an empty arrow.
Trust Boundary		**Object:** A closed shape drawn with a dashed or dotted line. **Represents:** A way to display different trust levels between objects.

Example: definition of the system and of the use cases

The Ankle Monitor Predictor of Stroke System:
AMPS is a home use medical device worn at night (or when resting) by patients considered at risk for a stroke. The AMPS system gathers medical readings that can be later analyzed by a medical professional. While the system can help predict a patient's risk of experiencing a stroke, it does not alert—and is not intended to alert—if a stroke is imminent or occurring.

- Period of expected use: One to three months
- Medical capability: Diagnostic only
- Device invasiveness: Low (easily removable, like a wristwatch)

AMPS Core Use Case:
Alice has been informed by her doctor, based on her family history and several other risk factors, that she is at increased risk of experiencing a stroke. To gain further insight and determine a treatment plan, her doctor has instructed her to take the AMPS system home and wear it when she sleeps to take readings. She is also directed to install a companion app on her phone that will connect to the AMPS system (via Bluetooth) and upload the readings every day to the AMPS cloud service, where they will be analyzed by an automated algorithm. Alice's doctor will check the results after the first week to identify any immediate causes of concern, and they will schedule a follow-up consult in two months.

Example: core technology

AMPS Core Technology:

- A Bluetooth Low Energy (BLE)-enabled ankle monitor that takes physiological measurements from the patient
- A phone/tablet application (app) for patients to pair with their ankle monitor that will display readings and communicate with the cloud services
- AMPSCS: The Ankle Monitor Predictor of Stroke Cloud Service

Example: AMPS device

AMPS device:
AMPS is a health monitoring system worn on a patient's ankle when they are resting. It has the following specifications and capabilities:

- Weight: 0.13kg
- Power source: Lithium-ion battery recharged via universal serial bus (USB) C cable. Provides up to 96 hours of usage under normal circumstances
- On/off switch
- Physical Bluetooth pairing button
- Proprietary stroke-predicting sensor. Note: This is a fictional sensor that requires contact with a patient's skin.
- Heart rate monitor
- Body temperature sensor
- Bluetooth Low Energy (BLE) connectivity
- Onboard computer and flash storage that can store up to two weeks of patient data for later transmission

Example: patient app

Patient App:
There are two different versions of the patient app, one for Apple iOS, and another for Android devices. Both apps contain the following functionality:

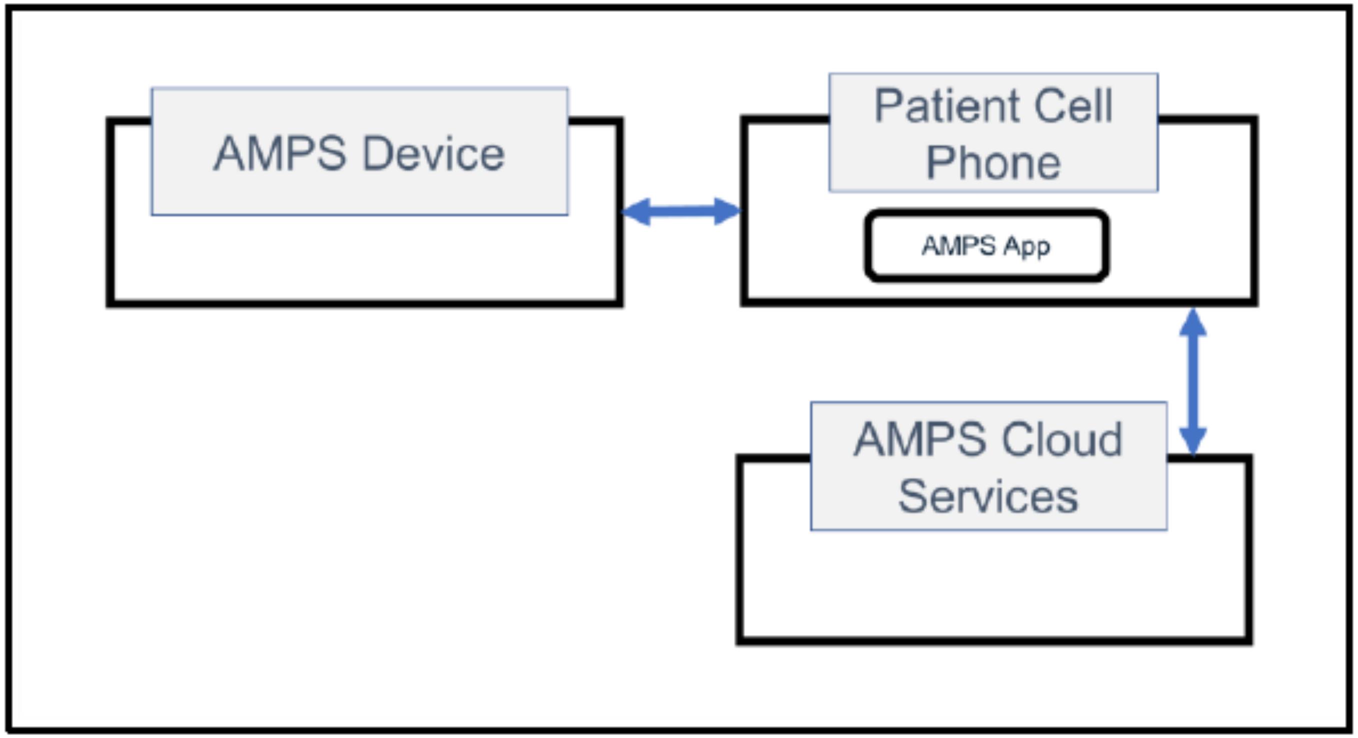
- The app is downloaded by the patient via Google Play or the Apple app store.
- It can pair with the AMPS device via Bluetooth.
- It contains an interface for a patient to create an account with the AMPS cloud services, register an AMPS device, and authorize clinicians to view their data.
- If the patient gives permission to the app, it will automatically connect to the AMPS device once a day and upload readings to the AMPSCS. If the patient does not give it permission, the app will store the data retrieved from the AMPS device until a manual upload is initiated. The amount of data transferred per upload is typically less than 1 megabyte a day.
- The app will display status information to the patient, including the last time the app synced with the AMPSCS, a log of the days the app was able to pull data from the AMPS device, and a log listing if the AMPS device was successfully collecting data.
- There is a device management screen that primarily focuses on diagnosing Bluetooth connection problems, and common issues that may prevent the AMPS device from collecting data. In addition:
    - The app can wipe patient data from the AMPS device.
    - The app can check for and update the firmware of the AMPS device with new versions.
    - The app can revert the AMPS device to factory default settings.
- If the device does not successfully sync to the cloud services once every 24 hours, an in-app notice will appear directing the patient to sync their data. After 72 hours have elapsed since a successful sync, the patient will be emailed an automatic reminder.

Example: cloud service

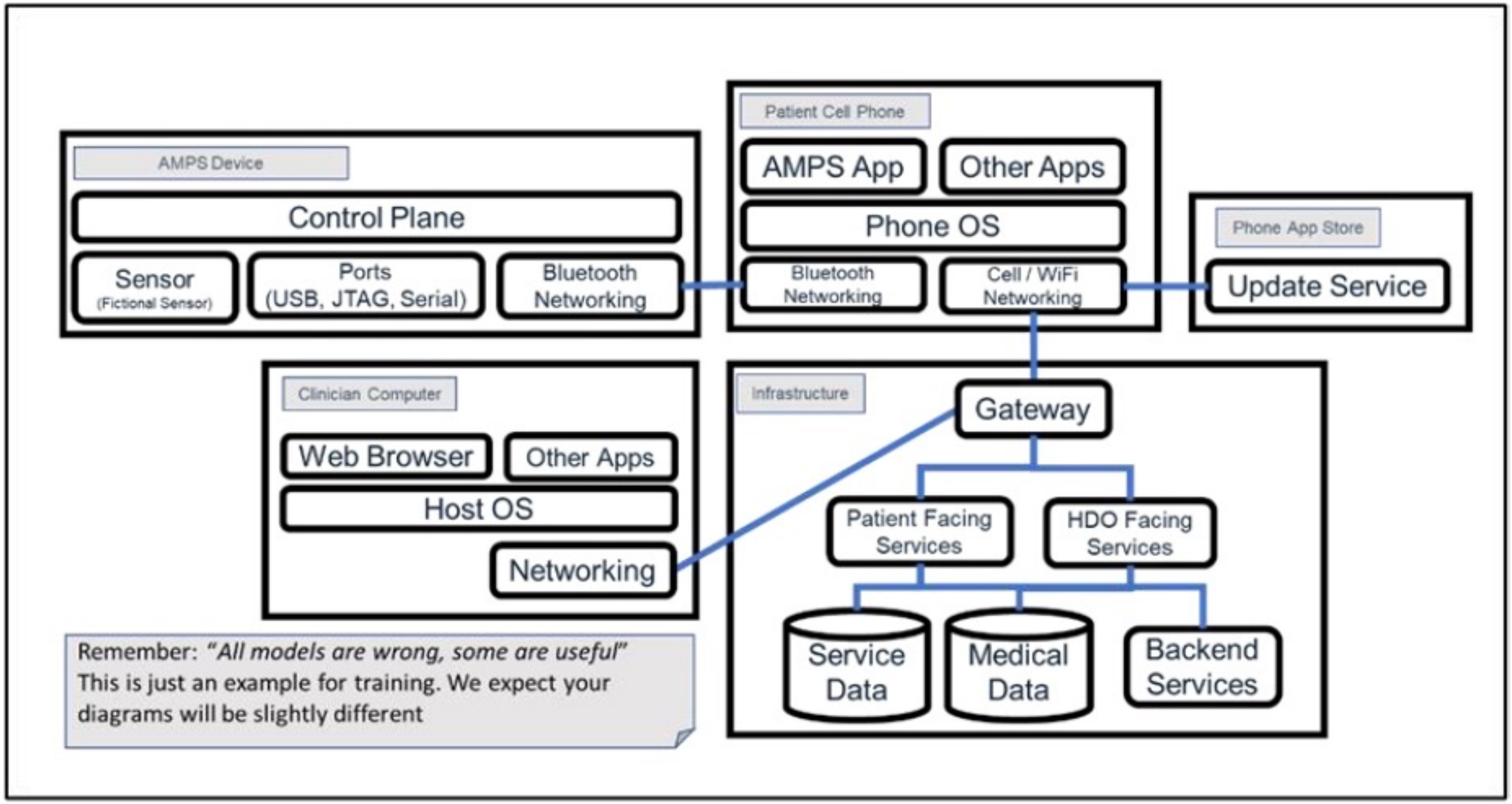
AMPS Cloud Service:
The AMPSCS is a collection of virtual machines hosted in a cloud infrastructure. It consists of the following functionality:

- An application gateway server to inspect and limit traffic going into the AMPSCS systems
- A set of backend services that perform analysis of the patient data
- A collection of patient-facing services that communicate with the patient app, provide a web portal for patients to register their AMPS device, and authorize clinicians to view their data
- A collection of health delivery organization (HDO)-facing services that provide a web portal for clinicians to create an account and access a patient's data
    - Clinicians' access to the portal using a web browser.
    - Authentication is provided via username and password.
    - Clinician service identifiers that clinicians can provide to patients so the patients can authorize them through the app.
    - The clinicians can view a summary of the patient's raw data and the analysis performed by the AMPSCS backend algorithms.
    - The ability for clinicians to download a patient's data via an encrypted zip file.

Example: high-level diagram



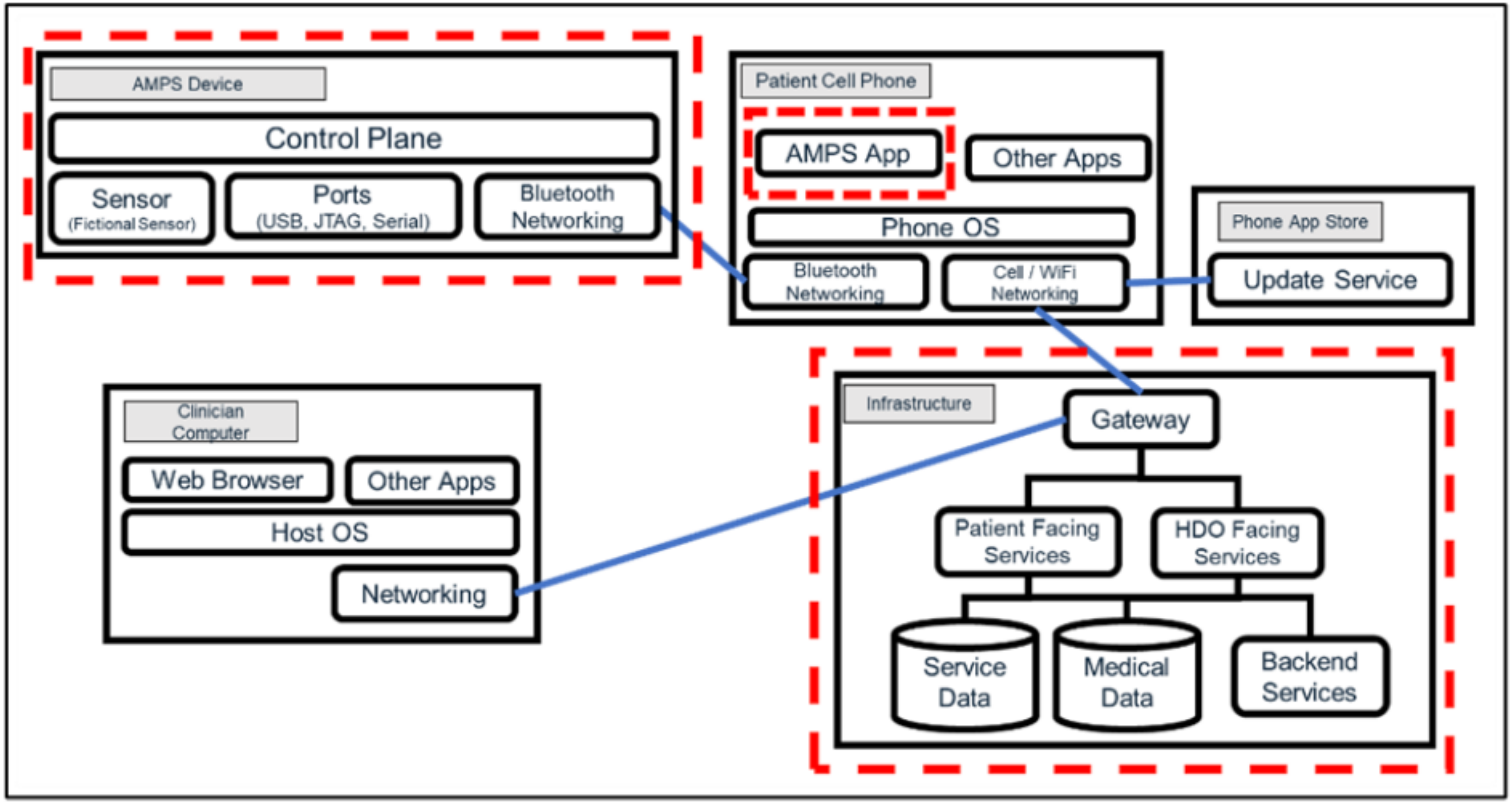
Example: detailed DFD



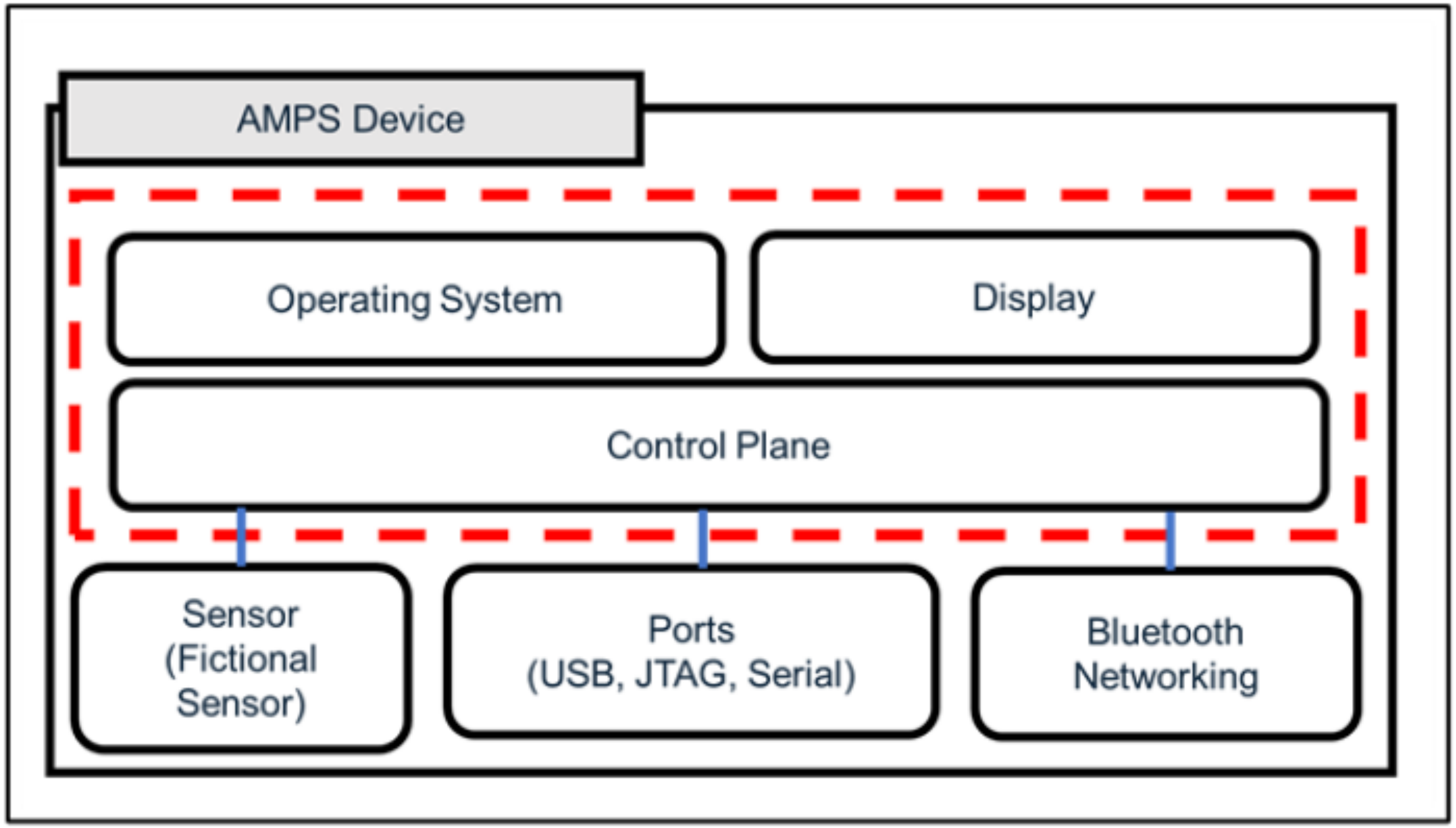
Trust boundaries

- Trust boundaries do not physically reside in a given organization’s system, but instead represent ideas and assumptions being made by the threat modeling team about how different entities interact.
- Trust boundaries help in later stages of the threat modeling process by identifying areas that require enhanced investigation.
- Trust boundaries help capture the thought process of the threat modeling team and can be used to help convey that information to external reviewers.

Example: trust boundaries



Example: trust boundaries within a device



Identification of threats step 2: threat identification

- There are several techniques:
  - STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege)
  - Attack trees
  - Kill Chains and Cyber Attack Lifecycles
  - ATT&CK Framework

STRIDE

STRIDE is a mnemonic that articulates six types of potential threats against a system.

STRIDE Element	***Description***	***Example***
Spoofing	Tricking a system into believing a falsified entity is a true entity	Using stolen or borrowed credentials to log on as another nurse
Tampering	Intentional modification of a system in an unauthorized way	Changing patient data to incorrect values
Repudiation	Disputing the authenticity of an action taken	Denying that a prescribed treatment has been provided to the patient
Information Disclosure	Exposing information intended to have restricted access levels	Health data is sent over an unencrypted Bluetooth connection
Denial of Service (DoS)	Blocking legitimate access or functionality of a system by malicious process(es)	A Bluetooth SpO2 sensor is flooded with bad pairing requests, preventing legitimate connections
Elevation of Privilege (EoP)	Gaining access to functions to which an attacker should not normally have access according to the intended security policy of the product	A patient uses a web portal vulnerability to see all patient data, rather than their own

STRIDE per element

STRIDE can be applied to the DFD elements or dataflow (“STRIDE per Element” approach).

This method is developed by analyzing which STRIDE threats tend to appear for individual DFD element types.

This approach creates a mapping where for a particular DFD element, there will be a list of STRIDE threats commonly associated with it.

Element	*Spoof*	*Tamper*	*Repudiate*	*Info Disclosure*	*DoS*	*EoP*
External Entity	X		X			
Process	X	X	X	X	X	X
Data Store		X	?	X	X	
Dataflow		X		X	X	

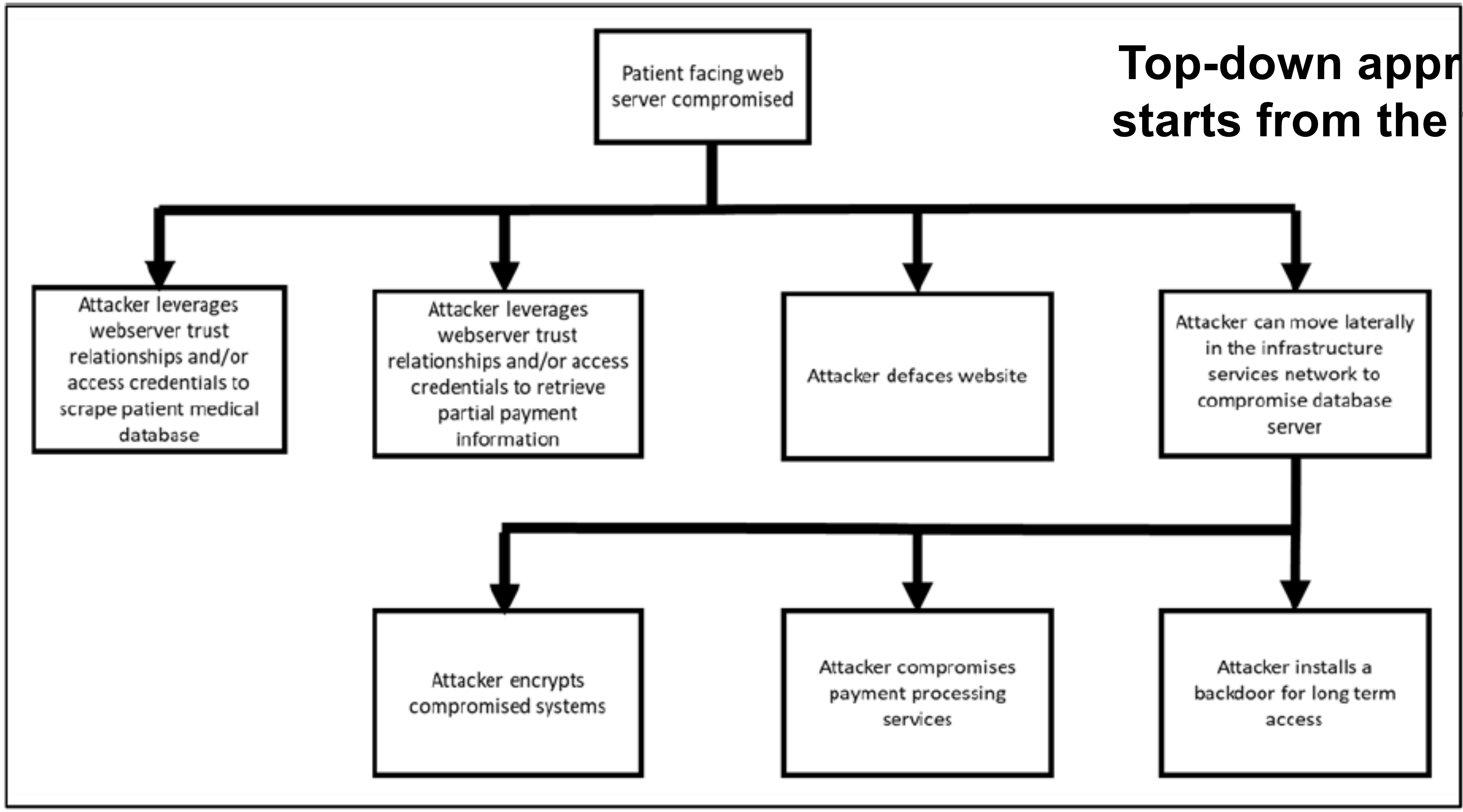
Example: STRIDE application

AMPS Component	Spoof	Tamper	Repudiate	Info	DoS	EoP
AMPS Device	1	2			3, 34, 35	4
AMPS App	5, 36	6		7	8	9, 37
App Store	10, 38	11		12	13	14
AMPSCS	15, 39, 40	16,41	17, 42, 43, 44	18, 45	19, 46, 47, 48	20, 49, 50
Clinician Computer	21, 51, 52	22		23	24, 53	25
Dataflow: Bluetooth				26	27, 54	
Dataflow: Cell/Wi-Fi Network		28		29	30	
Dataflow: Clinician Computer Internet		31		32	33	

Example: STRIDE application

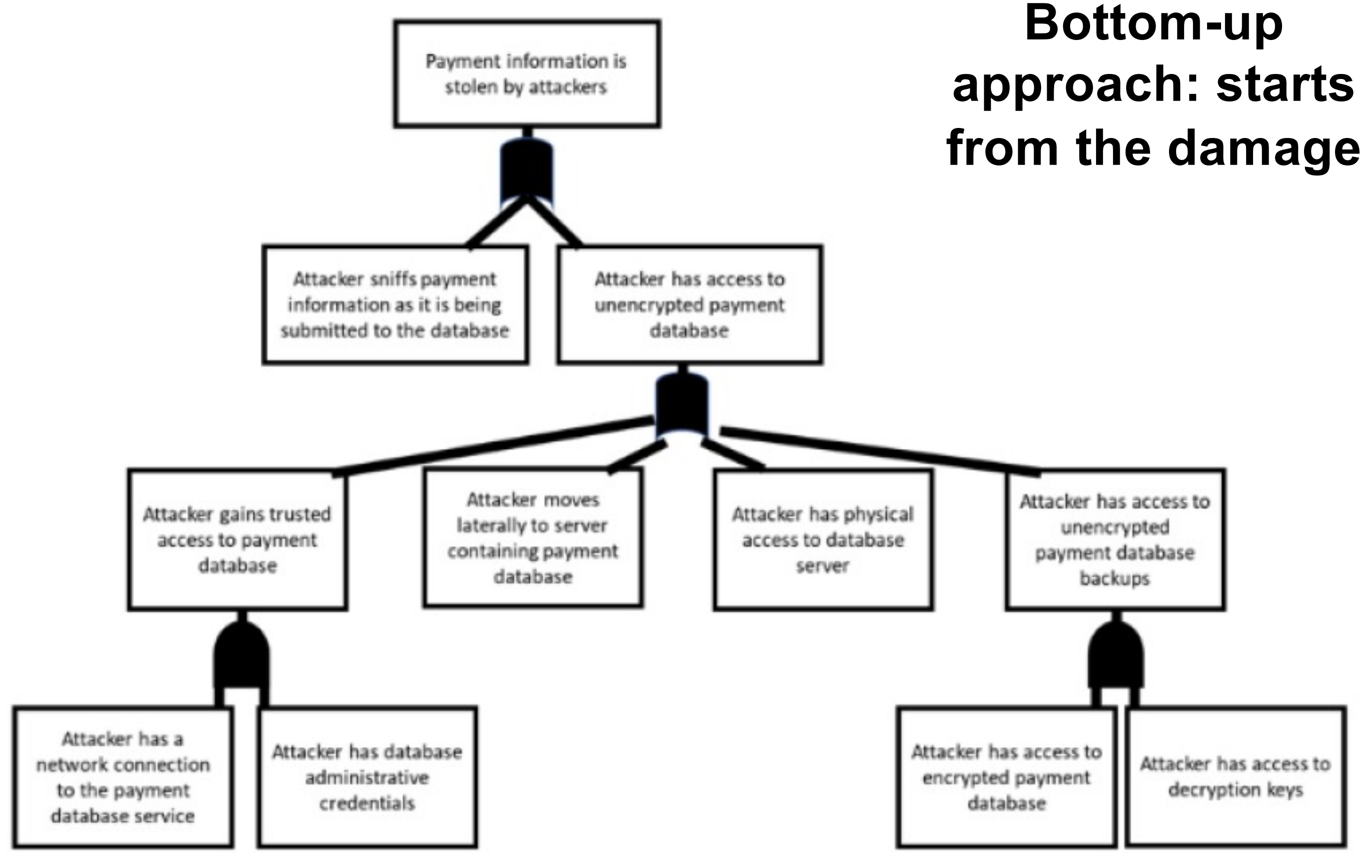
Reference ID	***STRIDE Type***	***Description***
1	Spoof	An attacker could pretend to be an authorized phone app to obtain readings from the device
2	Tamper	Control plane could be attacked and given incorrect readings
3	DoS	Invalid input could cause device to crash
4	EoP	Device could be hacked, and software could be installed to perform other actions (such as make it part of a botnet, enable lateral movement, etc.)
34	DoS	Software could be corrupted
35	DoS	Battery could be drained more rapidly than normal

Attack trees



Top-down approach: starts from the threat

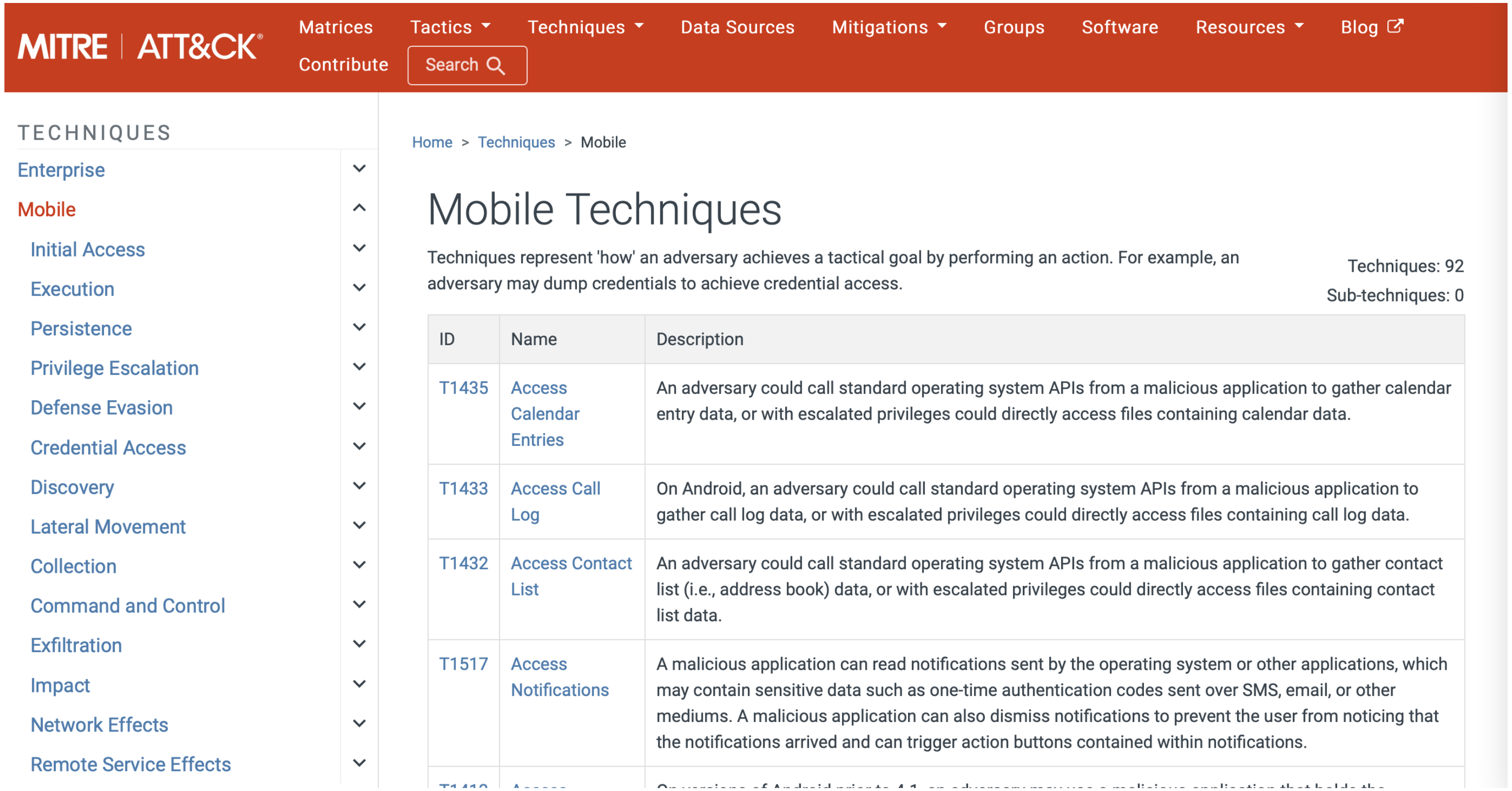
Attack trees



Bottom-up approach: starts from the damage

ATT&CK framework

ATT&CK is a public repository and framework for capturing and describing what attackers have done based on real-world data (https://attack.mitre.org)



MITRE | ATT&CK®

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Resources | Blog | Contribute | Search

TECHNIQUES

- Enterprise
- Mobile
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control
  - Exfiltration
  - Impact
  - Network Effects
  - Remote Service Effects

Home > Techniques > Mobile

Mobile Techniques

Techniques represent 'how' an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.

Techniques: 92

Sub-techniques: 0

ID	Name	Description
T1435	Access Calendar Entries	An adversary could call standard operating system APIs from a malicious application to gather calendar entry data, or with escalated privileges could directly access files containing calendar data.
T1433	Access Call Log	On Android, an adversary could call standard operating system APIs from a malicious application to gather call log data, or with escalated privileges could directly access files containing call log data.
T1432	Access Contact List	An adversary could call standard operating system APIs from a malicious application to gather contact list (i.e., address book) data, or with escalated privileges could directly access files containing contact list data.
T1517	Access Notifications	A malicious application can read notifications sent by the operating system or other applications, which may contain sensitive data such as one-time authentication codes sent over SMS, email, or other mediums. A malicious application can also dismiss notifications to prevent the user from noticing that the notifications arrived and can trigger action buttons contained within notifications.

Scoring

IEEE Std 11073-40101-2020
Health informatics—Device interoperability
Part 40101: Foundational—Cybersecurity—Processes for vulnerability assessment

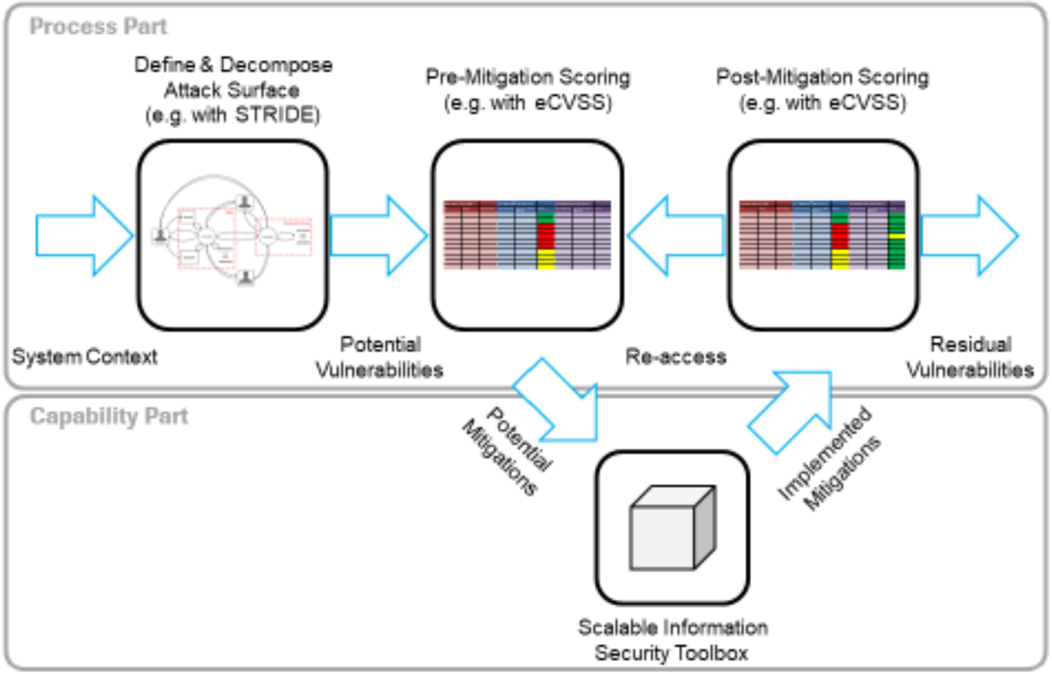


Figure 1—Vulnerability assessment workflow

Assessment of impact and likelihood

PROBABILITY OF OCCURENCE	SEVERITY OF HARM				
	Negligible Minor injury or property damage	**Minor** Limited injury or property damage	**Serious** Medically reversible injury or significant property damage	**Critical** Permanent injury or serious property damage	**Catastrophic** Life-threatening injury or catastrophic property damage
Frequent Happens with almost every use of the device	CAPA	UNACCEPTABLE	UNACCEPTABLE	UNACCEPTABLE	UNACCEPTABLE
Probable Occurs the majority of times but not with every use	CAPA	CAPA	UNACCEPTABLE	UNACCEPTABLE	UNACCEPTABLE
Occasional Occurs with increased frequency	ACCEPTABLE	CAPA	CAPA	UNACCEPTABLE	UNACCEPTABLE
Remote More than one occurrence per year but still unlikely	ACCEPTABLE	ACCEPTABLE	CAPA	UNACCEPTABLE	UNACCEPTABLE
Improbable Less than one occurrence per year; isolated events	ACCEPTABLE	ACCEPTABLE	ACCEPTABLE	CAPA	CAPA

embedded Common Vulnerability Scoring System - eCVSS

- The assessment has to be done before and after mitigation measures are put in place
- Even in the case of security/privacy by design the mitigation measures are not considered in the first assessment
- Two-level assessment:
  - System-wide level (system-wide metric): Represents the system requirements for a confidentiality, integrity, and availability (CIA) triad that are set once for the product and then applied to all vulnerabilities
  - Vulnerability level
    - base metric: intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.
    - environmental metric: the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

eCVSS system wide metric

System-wide metric	Metric description	Metric value	Value description	Numeric
Confidentiality Requirement (CR)	Enables the analyst to customize the score depending on the importance of the affected target device to the organization, measured in terms of confidentiality, integrity, and availability.	Undefined	N/A	1.000
		Low (L)	Loss of [confidentiality | integrity | availability] is likely to have only a limited adverse effect on the organization or users of the device.	0.500
Integrity Requirement (IR)		**Medium** (A)	Loss of [confidentiality | integrity | availability] is likely to have a serious adverse effect on the organization or users of the device.	1.000
Availability Requirement (AR)		**High** (H)	Loss of [confidentiality | integrity | availability] is likely to have a catastrophic adverse effect on the organization or users of the device.	1.510

eCVSS base metric (1/2)

Base metric	Metric description	Metric value	Value description	Numeric
Access Vector (AV)	How the vulnerability is exploited. The more remote the attacker can be to attack a system, the greater the score.	Undefined	N/A	0.000
		Local (L)	Attacker requires physical access to the device.	0.395
		Adjacent (A)	Attacker requires access to a broadcast or very short-range communications.	0.646
		Network (N)	Attacker requires access to WAN or Internet.	1.000
Access Complexity (AC)	The complexity of the attack required to exploit the vulnerability once an attacker has gained access to the system. The lower the required complexity, the higher the vulnerability score.	Undefined	N/A	0.000
		Low (L)	Specialized access conditions or extenuating circumstances do not exist.	0.710
		Medium (M)	The access conditions are somewhat specialized.	0.610
		High (H)	Specialized access conditions exist.	0.350
Authentication (Au)	The strength of the authentication process used to exploit the vulnerability.	Undefined	N/A	0.000
		None (N)	Authentication is not required to access and exploit the vulnerability.	0.704
		Single (S)	Authentication is easily defeated or uses a weak method for vetting. Examples include — Storing or transmitting of credentials in plain text — Fixed (i.e., hard coded) credentials — Automatic trust based on device type	0.560
		Multiple (N)	Authentication employs industry's best practice for vetting the authenticity of the user or device. Examples include: — Storing of hashed credentials only — Multiple levels of authentication — Enforced unique credentials	0.450

eCVSS base metric (2/2)

Base metric	Metric description	Metric value	Value description	Numeric
Confidentiality Impact (C)	The impact to confidentiality of a successfully exploited vulnerability.	Undefined	N/A	0.000
		None (N)	There is no impact to the confidentiality of the system.	0.000
		Partial (P)	There is considerable information disclosure. Access to some system files is possible; however, the attacker does not have control over what is obtained, or the scope of the loss is constrained.	0.275
		Complete (C)	There is total information disclosure, allowing all system files to be revealed.	0.660
Integrity Impact (I)	The impact to integrity of a successfully exploited vulnerability.	Undefined	N/A	0.000
		None (N)	There is no impact to the integrity of the system.	0.000
		Partial (P)	Modification of some system files or information is possible; however, the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.	0.275
		Complete (C)	There is a total compromise of system integrity.	0.660
Availability Impact (A)	The impact to availability of a successfully exploited vulnerability.	Undefined	N/A	0.000
		None (N)	There is no impact to the availability of the system.	0.000
		Partial (P)	There is reduced performance or interruptions in resource availability.	0.275
		Complete (C)	There is a total shutdown of the target system, rendering the system's principal functionality non-operational.	0.660

eCVSS environmental metric

Environmental metric	Metric description	Metric value	Value description	Numeric
Collateral Damage Potential (AV)	The potential for loss of life or physical assets through damage or theft of property or equipment. This metric may also measure economic loss of productivity or revenue. The greater the damage potential, the higher the vulnerability score.	Undefined	N/A	0.000
		None (N)	There is no potential for loss of life, physical assets, productivity, or revenue.	0.000
		Low (L)	A successful exploit of this vulnerability may result in slight physical damage, property damage, loss of revenue, or productivity.	0.100
		Low-Medium (LM)	A successful exploit of this vulnerability may result in moderate physical damage, property damage, loss of revenue, or productivity.	0.300
		Medium-High (MH)	A successful exploit of this vulnerability may result in significant physical damage, property damage, loss of revenue, or productivity.	0.400
		High (H)	A successful exploit of this vulnerability may result on catastrophic physical damage, property damage, loss of revenue, or productivity.	0.500
Awareness (Aw)	The ability of a vulnerability exploit to be detected by the system or its user. It is meant as an environment-specific indicator to lower the scoring as a result of an exploit being detected.	Undefined	N/A	1.000
		None (N)	Exploit cannot be detected by the user or the device.	0.000
		User (U)	Exploit is detectable by the user, e.g., the device case has obvious alterations, tampering is evident.	0.510
		Automatic (A)	Exploit is detectable by the device (either software or hardware).	0.680
		Complete (C)	Exploit is detectable by the user and the device.	0.840

eCVSS example

Device type		System-wide metrics			Threshold		
Name	Classification	Confidentiality Requirement	Integrity Requirement	Availability Requirement	Low-risk	Moderate-risk	High-risk
Insulin delivery device	Class IIb	Medium	High	Medium	<3.5	≥3.5	≥7.0

Potential vulnerability		Assessment			
Name	Category	Pre-mitigation vector	Pre-score	Post-mitigation vector	Post-score
Spoofing the Patient External Entity	Spoofing	ISE:Y AV:L AC:L Au:N C:C I:C A:C CDP:MH Aw:U	4.1	ISE:Y AV:L AC:M Au:M C:P I:P A:P CDP:LM Aw:U	2.9
Elevation by Changing the Execution Flow in Connected Device	Elevation of Privilege	ISE:Y AV:L AC:L Au:N C:N I:C A:N CDP:MH Aw:N	8.3	ISE:Y AV:L AC:H Au:M C:N I:P A:N CDP:L Aw:N	2.7
Elevation Using Impersonation	Elevation of Privilege	ISE:Y AV:L AC:L Au:N C:C I:C A:C CDP:MH Aw:U	4.1	ISE:Y AV:L AC:M Au:M C:P I:P A:P CDP:LM Aw:U	2.9
Connected Device May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation of Privilege	ISE:Y AV:A AC:H Au:N C:C I:C A:C CDP:MH Aw:N	8.1	ISE:Y AV:A AC:H Au:M C:P I:P A:P CDP:L Aw:N	4.9
Data Flow CD Read Wireless IP Device Configuration/Therapy Setting/Observation Is Potentially Interrupted	Denial of Service	ISE:N AV:A AC:L Au:N C:N I:N A:P CDP:L Aw:C	0.6	ISE:N AV:A AC:L Au:M C:N I:N A:P CDP:L Aw:C	0.5
Potential Process Crash or Stop for Connected Device	Denial of Service	ISE:N AV:A AC:H Au:N C:N I:N A:C CDP:L Aw:U	2.5	ISE:N AV:A AC:H Au:M C:N I:N A:C CDP:L Aw:U	2.3
Data Flow Sniffing	Information Disclosure	ISE:N AV:A AC:L Au:N C:C I:N A:N CDP:L Aw:N	6.5	ISE:N AV:A AC:M Au:M C:C I:N A:N CDP:L Aw:N	5.3
Potential Lack of Input Validation for Connected Device	Tampering	ISE:Y AV:A AC:M Au:N C:P I:P A:N CDP:LM Aw:N	6.6	ISE:Y AV:A AC:M Au:M C:P I:P A:N CDP:LM Aw:N	5.9
Spoofing the Connected Device Process	Spoofing	ISE:N AV:A AC:M Au:N C:C I:N A:N CDP:L Aw:N	6.1	ISE:N AV:A AC:H Au:M C:C I:N A:N CDP:L Aw:N	4.7
Spoofing the Controller Insulin Pump Process	Spoofing	ISE:Y AV:A AC:M Au:N C:N I:C A:N CDP:MH Aw:N	8.7	ISE:Y AV:A AC:H Au:M C:N I:C A:N CDP:L Aw:U	3.2
Elevation by Changing the Execution Flow in Controller Insulin Pump	Elevation of Privilege	ISE:Y AV:L AC:L Au:N C:N I:C A:N CDP:MH Aw:U	4.1	ISE:Y AV:L AC:H Au:M C:N I:P A:N CDP:L Aw:U	1.3

Mitigation measures

- There are four main strategies for addressing threats:
  - Eliminate
  - **Mitigate**
  - Accept
  - Transfer
- Major mitigation measures:
  - Protect
  - Detect
  - Respond
  - Recover

Mitigation measures

IEEE 11073 - 40102

Table 1—Mitigation categories, security capabilities, mitigation techniques, and design principles

Mitigation category (based on NIST cybersecurity framework [B15])		Security capability (based on IEC TR 80001-2-2 [B8])	Mitigation technique and design principle	S	T	R	I	D	E
Identify		Node authentication Personal authentication	Authentication	X				X	
			Digital signatures	X	X	X			
Protect	Prevent	Authorization Health data de-identification Health data storage and confidentiality Health data integrity and authenticity Physical locks on device Automatic logoff Configuration of security features	Authorization		X		X	X	X
			De-identification				X		
			Do not store secrets	X	X		X		X
			Encryption				X		
			Filtering					X	
			Message authorization code		X				
			Physical tamper resistant		X		X		
			Protect secrets and secret data	X	X		X		X
	Limit	Software application hardening Security guidelines	Input sanitization		X		X		
			Input validation		X				
			Quality of service					X	
			Least privileges						X
			Throttling					X	
Detect		Audit Physical locks on device	Audit trail			X			
			Physical tamper evidence		X		X		
Respond		Malware detection and protection emergency access	End-user signalization	X	X		X	X	X
			Invalidate compromised security	X	X	X	X	X	X
Recover		Data backup and disaster recovery cybersecurity product updates	Re-establish security	X	X	X	X	X	X

Cybersecurity risk assessment matrix

3	NUMBER	STRIDE TYPE	THREAT	THREAT TREE	HARM	SEVERITY LEVEL	RISK LEVEL	MITIGATION MEASURES	LIKELIHOOD	RESIDUAL RISK
4	1	SPOOF	An attacker may impersonate NWKstation and try to establish RF connection with AlphaDBSipg	the attacker may program AlphaDBSipg with overstimulation	temporary overstimulation side effects (e.g.dyskinesias)	negligible	acceptable	- The connection to the AlphaDBSipg requires a that AlphaDBSipg is woken-up by inductive coupling with the AlphaDBSpat which has to be placed in contact with the patient. Wireless connection cannot be established without starting it by touching the patient. - After waking up, the AlphaDBSipg has to establish a trusted communication with the AlphaDBSpat, which share with the AlphaDBSipg an ID code, which is hardcoded in the AlphaDBSipg and is the same for all the AlphaDBSpat. - After a trusted communication with the AlphaDBSpat has been established then the NWKstation can request to start a communication and stop the one in place with the Alpha DBS pat. To do that the NWKstation share with the AlphaDBSipg an ID code, which is hardcoded in the AlphaDBSipg and is the same for all the NWKstation. - the RF communication protocol is a proprietary protocol	Unlikey: - the attacker has to be near the patient, and has to use the poatient's AlphaDBSpat to wake up the AlphaDBSipg - the attacker has to be close to the patient (less than 10 m) to set the RF communication - the attacker has to know or decode the ID code for trusted connection - the attacker has to know or decode the proprietary protocol	ACCEPTABLE
5	2	SPOOF		the attacker may program AlphaDBSipg with suboptimal stimulation	temporary return of PD symptoms	negligible	acceptable	- The connection to the AlphaDBSipg requires a that AlphaDBSipg is woken-up by inductive coupling with the AlphaDBSpat which has to be placed in contact with the patient. Wireless connection cannot be established without starting it by touching the patient. - After waking up, the AlphaDBSipg has to establish a trusted communication with the AlphaDBSpat, which share with the AlphaDBSipg an ID code, which is hardcoded in the AlphaDBSipg and is the same for all the AlphaDBSpat. - After a trusted communication with the AlphaDBSpat has been established then the NWKstation can request to start a communication and stop the one in place with the Alpha DBS pat. To do that the NWKstation share with the AlphaDBSipg an ID code, which is hardcoded in the AlphaDBSipg and is the same for all the NWKstation. - the RF communication protocol is a proprietary protocol	Unlikely: - the attacker has to be near the patient, and has to use the poatient's AlphaDBSpat to wake up the AlphaDBSipg - the attacker has to be close to the patient (less than 10 m) to set the RF communication - the attacker has to know or decode the ID code for trusted connection - the attacker has to know or decode the proprietary protocol	ACCEPTABLE

Traceability matrix

Traceability among requirements, specifications, identified hazards and mitigations, and Verification and Validation testing.

Mitigation measure	System requirement	Test case	Test execution	Test result	Issues