SAND5G

https://sand5g-project.eu/

Cybersecurity in Digital Health Solutions

This project has received funding from the DIGITAL EUROPE (DIGITAL) programme under Grant Agreement No 101127979

wings.

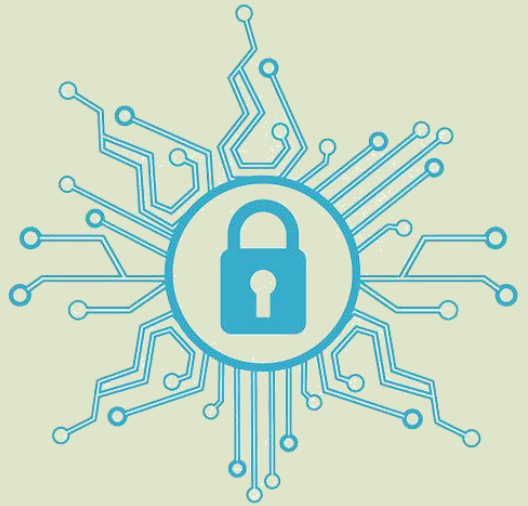
Table of Contents:

General Concepts

Introduction to Cybersecurity

Cybersecurity encompasses the frameworks, controls, and operational mechanisms designed to safeguard digital assets like data, systems, networks, and services, from malicious activity.

In modern infrastructures, especially those running on distributed, cloud-native, and 5G-enabled architectures, cybersecurity **is not a support function but a core resilience pillar.**



Main targets of cybersecurity:

- Protection of data confidentiality, integrity, and availability
- Detection and mitigation of cyber threats and anomalies
- Prevention of unauthorized access and operational disruption
- Recovery and continuity planning at scale

Core Cybersecurity Technologies:

- **5G Network Security** – Protects next-generation mobile networks through slicing security, zero-trust architectures, strong authentication, and improved encryption to handle massive device connectivity.
- **Firewalls & Network Security Tools** – Control and filter traffic to block unauthorized access and detect suspicious network behavior.
- **Endpoint Detection & Response (EDR)** – Monitors devices for malicious activity using behavioral analytics and automated threat response.

Introduction to Digital Health

Digital health integrates ICT, **medical devices**, **sensors**, **cloud systems**, and **data analytics** to streamline workflows, improve patient outcomes, and enable continuous, data-driven care delivery. By enabling remote monitoring, telemedicine, and real-time decision support, digital health modernizes clinical practice, increases accessibility, and drives a more patient-centered care model.

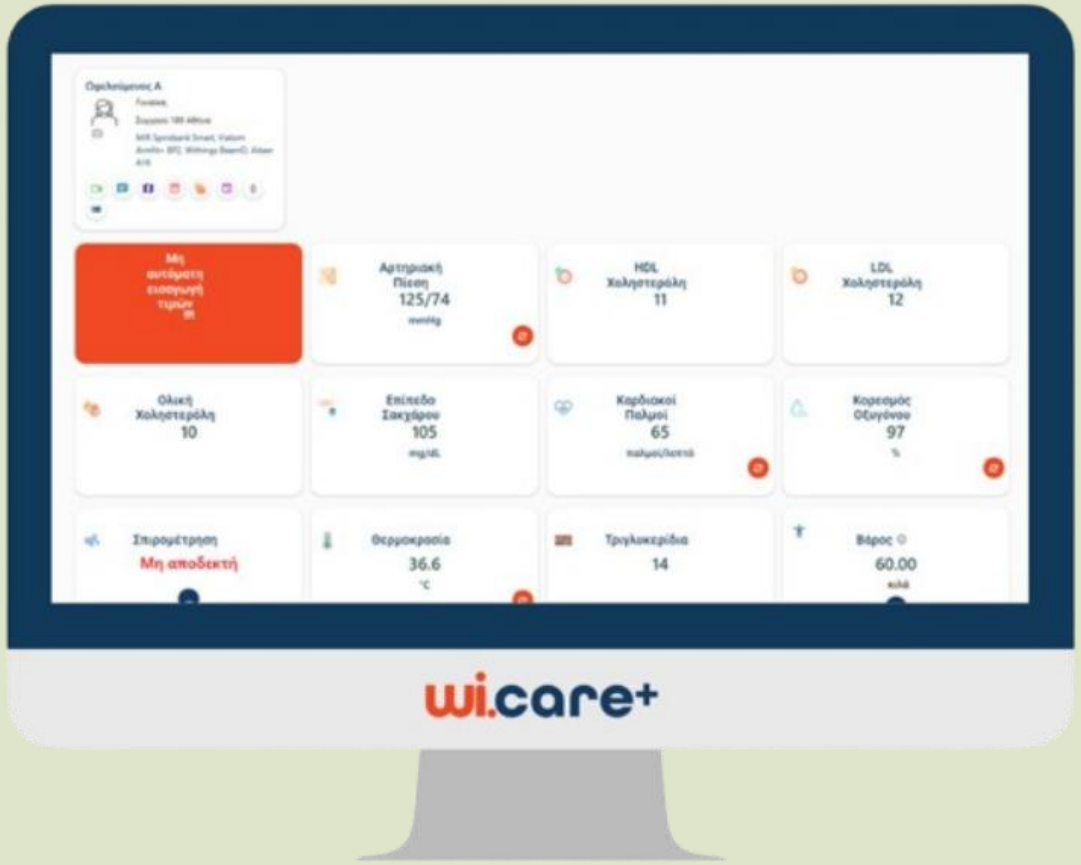
Main categories include:

Introduction to Digital Health

Platforms like **wi.care+** operationalize end-to-end remote monitoring, telemedicine, and intelligent decision support in real time.

Core capabilities of wi.care+:

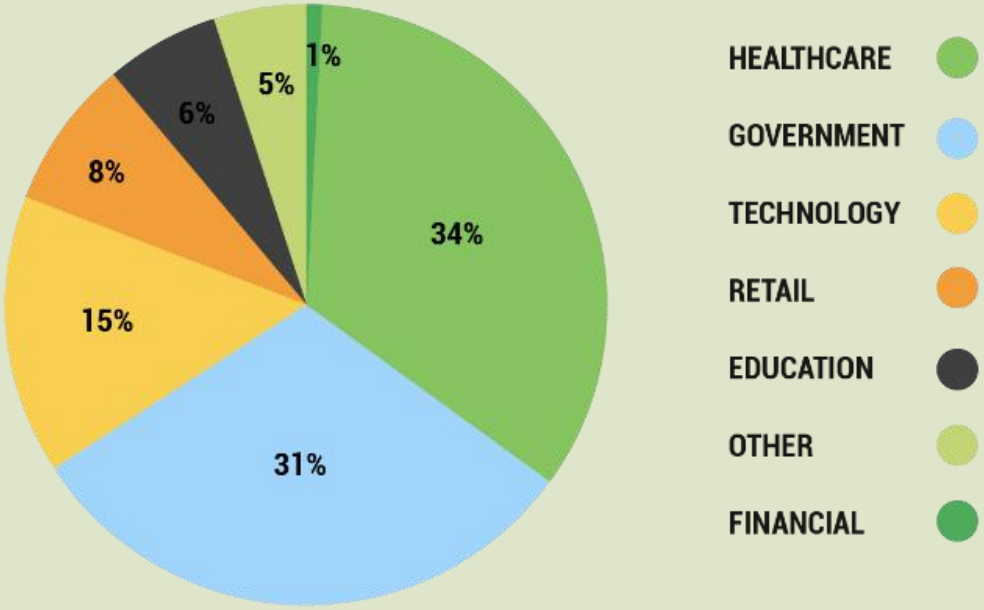
- **Continuous Vital-Sign Monitoring** through smart, connected medical devices
- **Real-Time Alerts & Clinical Dashboards** for rapid intervention and workflow optimization
- **Remote Patient Monitoring** enabling safer discharge, home care, and reduced readmissions
- **Cloud-Enabled Data Exchange** with secure, encrypted communication channels
- **AI-Driven Insights** supporting early detection of critical events
- **Role-Based Access & Secure Authentication** ensuring controlled access to sensitive health data



Cybersecurity & Digital Health

Operating 24 hours a day, **digital health platforms** are easy and primer targets for cyberattacks. **Electronic records systems and fleets of medical devices** are particularly vulnerable to attack. Increased significantly after the Covid-19 pandemic.

Number Of Records Breached By Industry



- Over a 2-year period (Jan 2021–Mar 2023), the health sector saw **215** publicly reported cyber-incidents in the EU
- Criminals usually demand **10%** of the health organization's or system's annual revenue.
- According to ENISA (the EU Agency for Cybersecurity), **only 27%** of health-sector organizations surveyed had a *dedicated cybersecurity system.*

Cybersecurity failures in digital health can lead to service outages, clinical delays, non-compliance with regulations, and erosion of organizational credibility.
A robust cybersecurity posture safeguards patient trust, operational integrity, and the continuity of critical health services.

Risks and Threats

Data Lifecycle Risks in Digital Health

Digital health ecosystems generate and process **continuous** streams of **high-sensitivity data**.
There are 4 main steps of the data pipeline process:

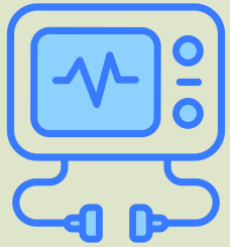
1. Data Acquisition → 2. Transmission → 3. Storage → 4. Access

Each step of the lifecycle introduces distinct cybersecurity exposures that must be proactively mitigated to safeguard clinical operations and regulatory compliance.

Most Dangerous Digital Healthcare Cyber Attacks

Phishing

Attackers trick users of healthcare platforms/staff into clicking malicious links or sharing credentials.
This often becomes the entry point for ransomware, data breaches, or system compromise.



Medical IoT Device Exploitation

Compromising connected clinical devices, sensors, or wearables.
Attackers exploit weak firmware, outdated patches, or insecure communication channels.
This can lead to false readings, device malfunction, or lateral movement inside hospital networks.

Data Breach

Unauthorized access to sensitive patient information, clinical records, or operational data.
Breaches typically occur through misconfigurations, weak authentication, or compromised accounts.
Impact includes GDPR penalties, loss of trust, and potential manipulation of medical data.

Ransomware

Malware encrypts hospital systems, EHRs, or telemonitoring platforms and demands payment.
Ransomware can halt clinical workflows, block access to dashboards, and disrupt patient care.
It's currently the most damaging attack type in healthcare worldwide, accounted for 54% of all cyber incidents in the health sector.

Most Dangerous Digital Healthcare Cyber Attacks

Man-in-the-Middle (MitM)

Attackers overwhelm online services with excessive traffic, causing outages.
DDoS can knock telemedicine portals, remote monitoring gateways, or 5G health APIs offline.
This leads to downtime, delayed treatments, and service unavailability during critical operations.

Distributed Denial of Service DDOS

Interception or alteration of data exchanged between devices, apps, and servers.
Attackers can eavesdrop on patient data or inject falsified vital-sign packets.
Often happens over insecure networks, outdated protocols, or compromised Wi-Fi/5G gateways.

Cloud Attacks

Targeting cloud infrastructure hosting digital health data and applications.
Includes misconfiguration exploits, API abuse, credential theft, and cross-tenant attacks.
Because healthcare platforms rely on secure cloud operations, cloud attacks pose high operational risk.

Cybersecurity Approaches

Core Cybersecurity Approaches: **Access Control & Authentication**

Effective access control is a foundational safeguard in digital health, ensuring that **only authorized identities** interact with critical clinical systems and sensitive patient data.
By enforcing **strict authentication** workflows and **granular privilege management**, organizations minimize exposure and reduce the blast radius of potential breaches.

Main Techniques:

- **Least Privilege:**
Users and services operate with the minimum access required to perform their functions.

- **Role-Based Access Control (RBAC):**
Structured permission models aligned to clinical, operational, and administrative roles.

- **Multi-Factor Authentication (MFA):**
Strong identity assurance for all privileged and remote-access accounts.

- **Secure API Authentication:**
Token-based mechanisms and rotating keys protecting machine-to-machine communication.

Core Cybersecurity Approaches: **Data Privacy & Encryption**

Safeguarding health data is both a regulatory obligation and a strategic trust enabler. A **privacy-by-design** approach ensures data is processed, stored, and transmitted with robust protections at every stage.

Core Practices

- **Data Minimization:** Only the necessary data fields are captured and retained.
- **Secure Data Processing:** Structured handling, sanitization, and protection of sensitive fields throughout the system.
- **End-to-End Encryption:** Encryption applied both ***in transit***—while data is being transferred between systems to protect it from interception—and ***at rest***—when data is stored on a device or server to prevent unauthorized extraction.
- **Key Management Controls:** Secure generation, storage, and rotation of encryption keys.

Core Cybersecurity Approaches: **Network & 5G Security**

Network security forms the **backbone of operational resilience** in digital health, particularly in ecosystems driven by IoT, cloud platforms, and 5G. Robust network segmentation and modern trust models limit attacker movement and preserve service continuity.

Strategic Network Controls

- **Segmentation:** Isolation of IoT devices, clinical systems, and cloud environments to prevent lateral movement.
- **Zero Trust Networking:** Continuous verification of every user, device, and packet—"never trust, always verify."
- **Protected Edge Gateways:** Hardened interfaces between device fleets and cloud infrastructure.
- **API & Transport-Layer Hardening:** Preventing injection, spoofing, or unauthorized access at protocol level.

5G-Specific Enhancements

- Stronger encryption and authentication at the RAN* and core network.
- Network slicing enabling dedicated, secure lanes for mission-critical digital health traffic.
- Lower latency supporting real-time monitoring and failover operations.

***Radio Access Network (RAN)**—the part of a mobile network that connects user devices to cellular base stations

Core Cybersecurity Approaches: **Cybersecurity Incident Detection**

Modern digital health infrastructures operate in a high-velocity environment where **early detection** is the decisive factor between a contained event and a full-scale operational disruption. Incident detection in this context relies on **continuous telemetry** across devices, applications, and networks, enabling **real-time insights into abnormal behaviors**.

Within a digital health workflow, every interaction—whether it originates from a wearable sensor, a telehealth session, or a backend API—generates **signals**. These signals are consolidated through logging pipelines and advanced analytics engines capable of **correlating patterns** that humans would miss. **Behavioral baselines** are established, allowing the system to recognize when something deviates from normal clinical operations, patient monitoring rhythms, or device activity cycles.

AI-enhanced detection frameworks further accelerate the process, automatically surfacing anomalies such as unusual data flows, compromised credentials, or sudden spikes in network activity. In practice, this means telemonitoring platforms gain early **warning indicators**, allowing security teams to intervene before patients or clinicians experience any service impact.

Core Cybersecurity Approaches: **Recovery & Continuous Improvement**

Resilience is not achieved through one-off actions; it requires continuous refinement of controls, processes, and system behavior. **Post-incident analysis** drives smarter defenses and stronger architectures.

Core Recovery Practices:

- **Robust Backup Strategy:** Automated, encrypted backups with verified integrity and recovery testing.
- **Failover Environments:** Hot/warm standby systems to restore operations without delay.
- **Post-Incident Review:** Root-cause analysis, threat modelling updates, and corrective actions.

Continuous Improvement Loop:

- Updated playbooks, retraining of staff, and tuning of detection models.
- Hardening of infrastructure and removal of systemic weaknesses.
- Closing the feedback loop to build a progressively stronger security posture.

Understanding: Multiple Choice Questions

Quiz 1

Which of the following best describes the purpose of cybersecurity in digital health?

a) To increase device connectivity speeds
b) To safeguard data, systems, and services from malicious activity
c) To reduce hospital operational costs
d) To improve medical device battery life

Quiz 1

Which of the following best describes the purpose of cybersecurity in digital health?

~~a) To increase device connectivity speeds~~
b) To safeguard data, systems, and services from malicious activity
~~c) To reduce hospital operational costs~~
~~d) To improve medical device battery life~~

Why: Cybersecurity protects digital health platforms from unauthorized access, attacks, data loss, and service disruption.

Quiz 2

What does the principle of “least privilege” mean?

a) Everyone receives the same access to simplify workflows
b) Users get temporary access during emergencies
c) Users only receive the minimum permissions needed for their role
d) Access is granted only to administrators

Quiz 2

What does the principle of “least privilege” mean?

~~a) Everyone receives the same access to simplify workflows~~
~~b) Users get temporary access during emergencies~~
c) Users only receive the minimum permissions needed for their role 
~~d) Access is granted only to administrators~~

Why: “Least privilege” means each user gets only the access required to do their job. This reduces risk because a compromised account cannot access everything in the system.

SAND5G

Quiz 3

What is the main risk associated with unsecured data transmission?

a) Reduced network performance
b) Loss of medical device battery
c) Possibility of interception or manipulation (MitM)
d) Difficulty sharing data between departments

Quiz 3

What is the main risk associated with unsecured data transmission?

~~a) Reduced network performance~~
~~b) Loss of medical device battery~~
c) Possibility of interception or manipulation (MitM) ✔
~~d) Difficulty sharing data between departments~~

Why: Unsecured transmission can allow attackers to intercept, read, or change health data while it moves between devices, apps, and servers. This is the core risk behind Man-in-the-Middle attacks.

Quiz 4

Which cyberattack overwhelms hospital or telehealth services with excessive traffic?

a) Phishing
b) Ransomware
c) Cloud attack
d) Distributed Denial of Service (DDoS)

Quiz 4

Which cyberattack overwhelms hospital or telehealth services with excessive traffic?

~~a) Phishing~~
~~b) Ransomware~~
~~c) Cloud attack~~
d) Distributed Denial of Service (DDoS) ✔

Why: A DDoS attack floods a service with excessive traffic until it becomes unavailable. In digital health, this can disrupt telemedicine portals, dashboards, or monitoring services.

Quiz 5

What is the role of encryption in digital health systems?

a) Speeding up patient data processing
b) Protecting data in transit and at rest from unauthorized access
c) Reducing storage requirements
d) Simplifying cloud operations

Quiz 5

What is the role of encryption in digital health systems?

~~a) Speeding up patient data processing~~
b) Protecting data in transit and at rest from unauthorized access ✔
~~c) Reducing storage requirements~~
~~d) Simplifying cloud operations~~

Why: Encryption makes data unreadable to unauthorized users, both when it is being transmitted and when it is stored. It protects sensitive patient information from exposure.

Quiz 6

What is the primary purpose of incident detection?

a) To slow down network requests
b) To identify abnormal or suspicious behavior early
c) To replace outdated medical devices
d) To automate hospital administration

Quiz 6

What is the primary purpose of incident detection?

~~a) To slow down network requests~~
b) To identify abnormal or suspicious behavior early
~~c) To replace outdated medical devices~~
~~d) To automate hospital administration~~

Why: Incident detection helps security teams identify suspicious activity before it becomes a major breach or operational disruption. Early detection is critical in healthcare because downtime can affect patient care.

Evaluation: Multiple Choice Questions

Quiz 1

Which situation represents a data breach in a digital health environment?

a) A device stops sending data due to low battery
b) An attacker gains unauthorized access to patient records
c) A scheduled system update
d) A temporary slowdown in the Wi-Fi network

Quiz 1

Which situation represents a data breach in a digital health environment?

~~a) A device stops sending data due to low battery~~
b) An attacker gains unauthorized access to patient records ✔
~~c) A scheduled system update~~
~~d) A temporary slowdown in the Wi-Fi network~~

Why: A data breach occurs when sensitive information is accessed without authorization. Patient records are protected health data, while low battery, scheduled updates, or Wi-Fi slowdown are operational issues.

Quiz 2

Which practice strengthens secure access control?

a) Using shared passwords between staff
b) Enabling multi-factor authentication (MFA)
c) Allowing broad access to avoid workflow delays
d) Disabling audit logs to reduce storage usage

Quiz 2

Which practice strengthens secure access control?

~~a) Using shared passwords between staff~~
b) Enabling multi-factor authentication (MFA) ✔
~~c) Allowing broad access to avoid workflow delays~~
~~d) Disabling audit logs to reduce storage usage~~

Why: MFA strengthens access control by requiring more than one proof of identity. Shared passwords and broad access reduce accountability and increase exposure.

Quiz 3

During a cybersecurity incident, what should be the first objective?

a) Enhancing the user interface
b) Buying new medical devices
c) Isolating the affected systems
d) Deleting all system data to reset the environment

Quiz 3

During a cybersecurity incident, what should be the first objective?

~~a) Enhancing the user interface~~
~~b) Buying new medical devices~~
c) Isolating the affected systems
~~d) Deleting all system data to reset the environment~~

Why: The first priority is containment. Isolating affected systems limits spread, protects remaining services, and preserves evidence for investigation and recovery.

Quiz 4

Which example indicates Medical IoT device exploitation?

a) A wearable sensor with outdated firmware being remotely accessed
b) A user forgetting their password
c) A scheduled cloud maintenance event
d) A doctor updating a patient’s file

Quiz 4

Which example indicates Medical IoT device exploitation?

a) A wearable sensor with outdated firmware being remotely accessed ✔
~~b) A user forgetting their password~~
~~c) A scheduled cloud maintenance event~~
~~d) A doctor updating a patient's file~~

Why: Remote access to a wearable with outdated firmware is a direct compromise of a connected medical device. The other options are normal user or maintenance activities.

Quiz 5

Which action aligns with continuous improvement after an incident?

a) Ignoring minor alerts to save time
b) Updating detection models and refining playbooks
c) Shutting down all monitoring systems permanently
d) Granting all users admin access for flexibility

Quiz 5

Which action aligns with continuous improvement after an incident?

~~a) Ignoring minor alerts to save time~~
b) Updating detection models and refining playbooks ✔
~~c) Shutting down all monitoring systems permanently~~
~~d) Granting all users admin access for flexibility~~

Why: Continuous improvement means learning from the incident, then updating detection rules, response playbooks, and controls so the same weakness is not repeated.

Quiz 6

What is a key advantage of 5G network slicing for digital health?

a) Reducing electricity consumption in hospitals
b) Providing dedicated, secure lanes for mission-critical health traffic
c) Allowing unlimited public access to the hospital network
d) Eliminating the need for encryption

Quiz 6

What is a key advantage of 5G network slicing for digital health?

~~a) Reducing electricity consumption in hospitals~~
b) Providing dedicated, secure lanes for mission-critical health traffic ✔
~~c) Allowing unlimited public access to the hospital network~~
~~d) Eliminating the need for encryption~~

Why: 5G network slicing creates dedicated logical network segments for critical health traffic, improving isolation, reliability, and security.