RIT Croatia

DIG HEALTH

Telemedicine Foundations: Technical Requirements for Telemedicine Implementation

DigHealth –

Micro-credentials in digital health for Ethiopia and Somalia

Proj. Ref. Num. 101179425

Capacity Building in the field of Higher Education

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Overview: Why Technical Requirements Matter

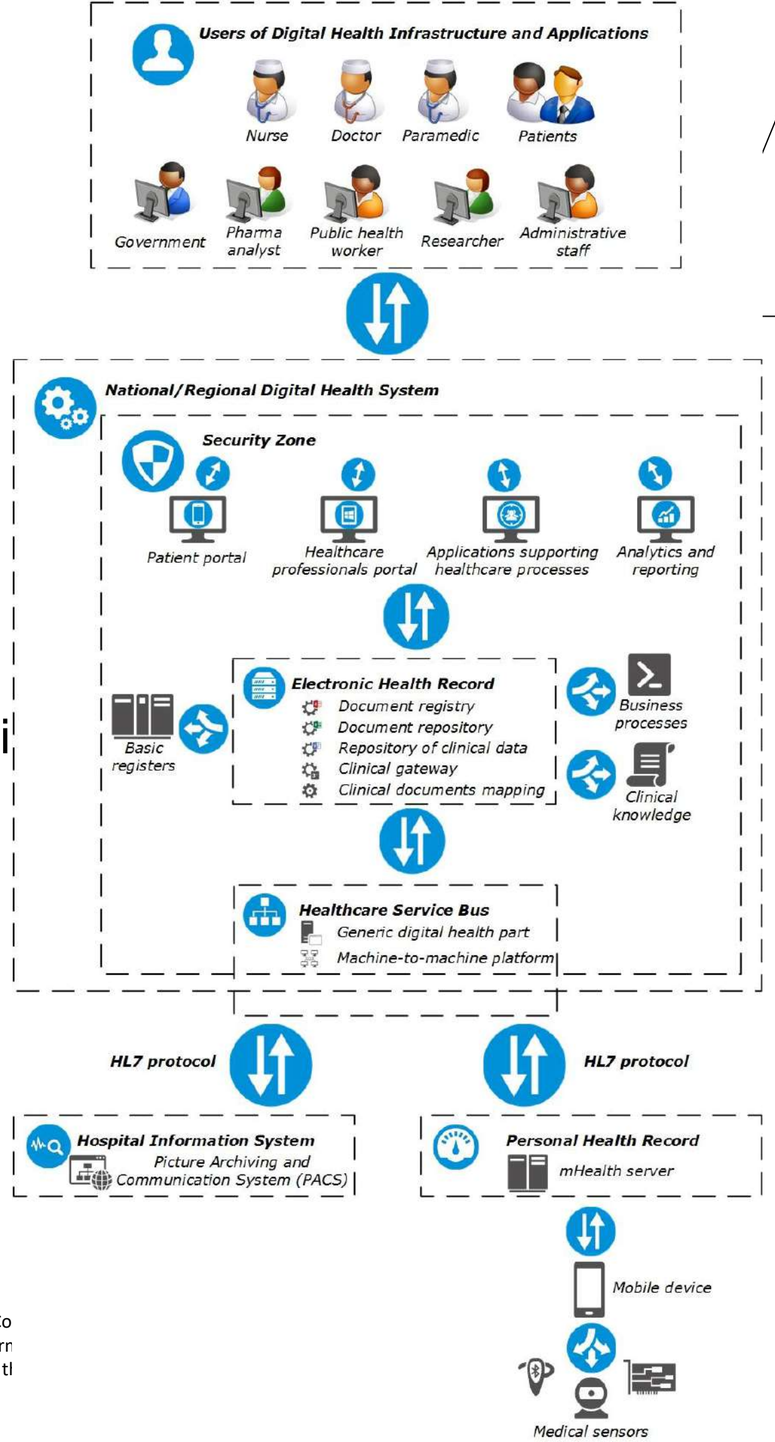
Ensures safe, effective, and reliable telemedicine services.
Impacts quality of care, privacy, and legal compliance.
Sets foundation for scalable, sustainable virtual healthcare.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Core Digital Infrastructure

High-Speed Internet: Essential for real-time audio/video connections.
Network Technologies: Broadband, 4G/5G, Wi-Fi; redundancy i critical.
Connectivity Testing/Monitoring: Prevents disruptions and improves reliability.

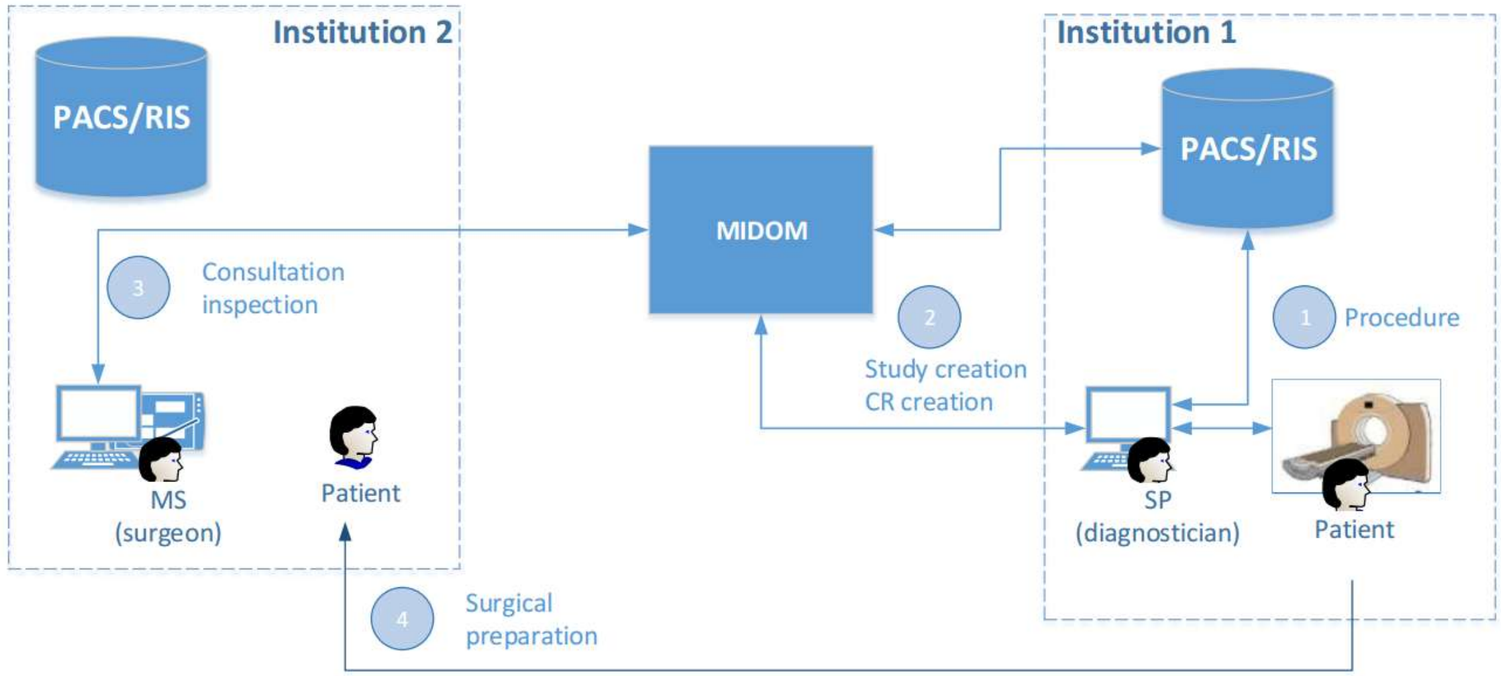


Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

End-User Hardware & Devices

For Patients: Smartphones, tablets, computers; sometimes wearables or home monitoring devices.
For Providers: Desktop computers, webcams, microphones, specialized diagnostic equipment (CT, MRI, ECG, etc). IMPORTANT: IEC 60601 Certification for Medical Electrical Equipment (see next slide)
Compatibility: Devices must support required software/apps.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

IEC 60601 Certification for Medical Electrical Equipment

Devices such as electrocardiogram (ECG) machines, ventilators, defibrillators, and ultrasound equipment rely on complex electrical systems to function safely and effectively.
IEC 60601 certification is essential for medical electrical equipment manufacturers to ensure that their products meet the stringent safety and performance standards required by regulatory bodies worldwide.
Compliance with this standard demonstrates a commitment to protecting patients from potential harm and provides assurance that devices will operate as intended, even in critical situations.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Regulatory Context

The International Electrotechnical Commission (IEC) has developed the IEC 60601 series of standards to address the unique electrical safety requirements for medical equipment. These standards cover design, construction, and testing aspects of medical electrical equipment to ensure that they do not pose a risk to patients or operators.
In many countries, regulatory authorities require medical devices to meet specific safety regulations before being released into the market.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

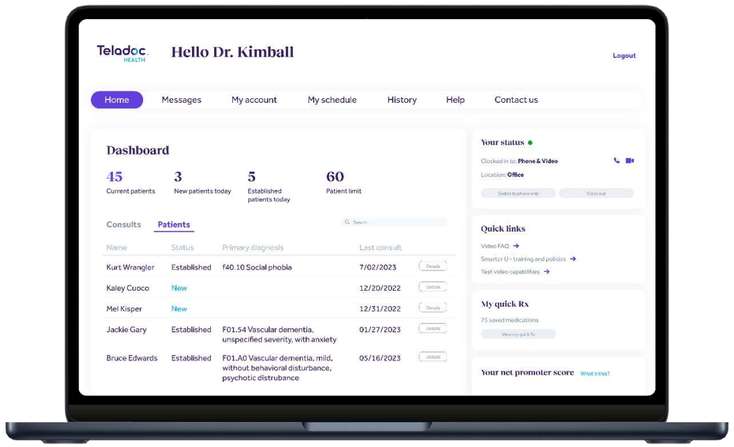
Telemedicine Software Platforms

Functions: Secure video conferencing, chat portals, file-sharing, appointment scheduling.
Features: HIPAA/GDPR-compliant (separate lecture), intuitive interface, EHR integration, multi-language support.
Selection Considerations: Ease of use, scalability, technical support, interoperability.

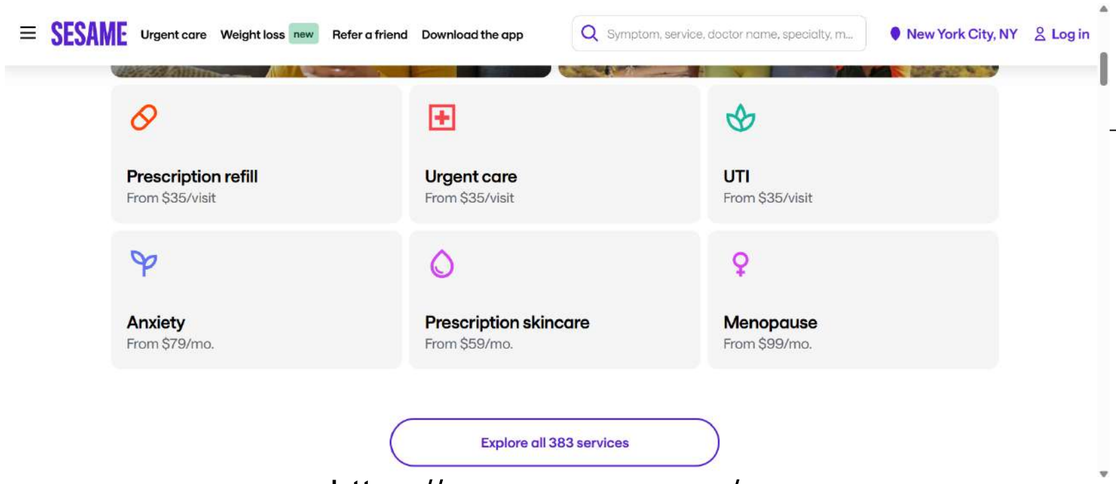
Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Telemedicine Software Platforms



https://www.teladochealth.com



https://sesamecare.com/

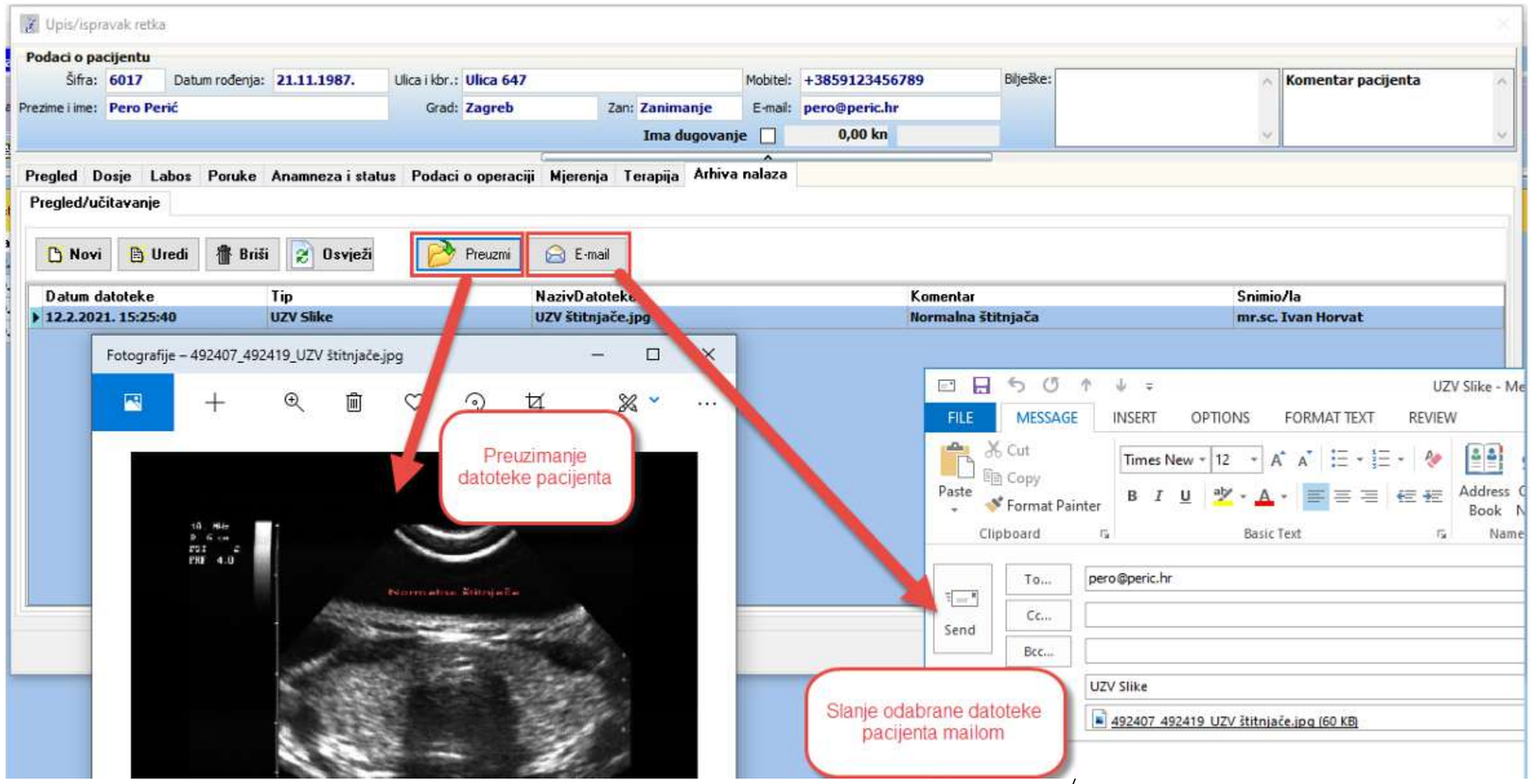
https://plushcare.com/

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Electronic Health Records (EHR) & Integration

Secure storage & access for patient data.
Seamless sharing with authorized providers, labs, and pharmacies.
Interoperability standards promote communication between disparate systems.



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Internet of Medical Things (IoMT) Devices

Examples: Remote stethoscopes, glucometers, BP monitors, ECG, pulse oximeters.
Functions: Real-time data, continuous monitoring, alert generation.
Requirements: Device pairing, calibration, user instruction, secure data transmission.

Co-funded by the European Union

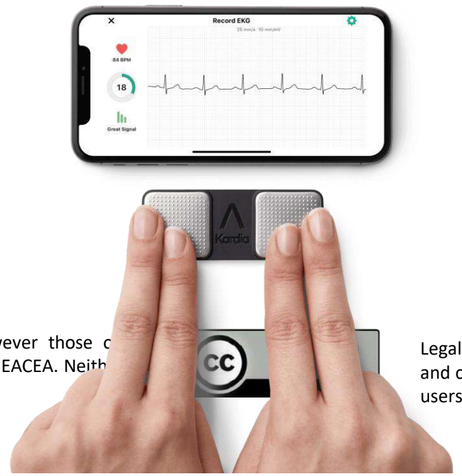
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

IoMT Wearable Devices

Omron HeartGuide: A wearable blood pressure monitor that looks like a smartwatch but can take clinical-grade blood pressure readings throughout the day

Dexcom G6: A continuous glucose monitoring system for diabetics that uses a small sensor inserted under the skin to provide real-time glucose readings every 5 minute

AliveCor KardiaMobile: A pocket-sized ECG device that can record medical-grade ECGs in just 30 seconds, detecting atrial fibrillation and other heart rhythm abnormalities

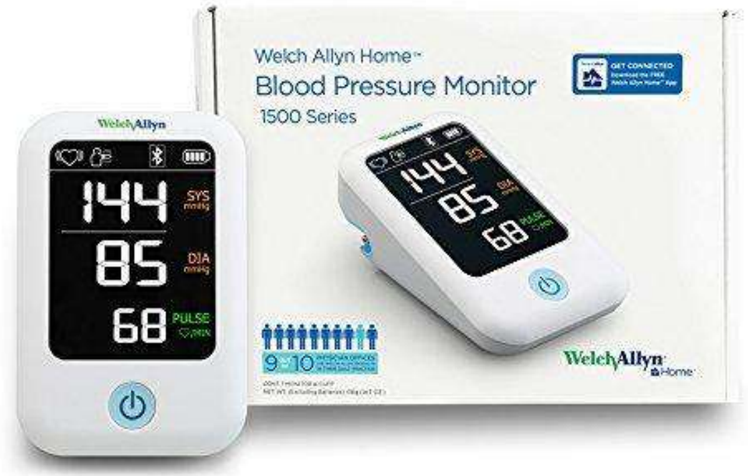


Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those o
author(s) only and do not necessarily reflect those of the European Union or EACEA. Neith
European Union nor the granting authority can be held responsible for them.

IoMT Wearable Devices

Bluetooth-enabled blood pressure monitors, scales, and glucometers: These devices connect to a cellular gateway to transmit health data through cellular networks.



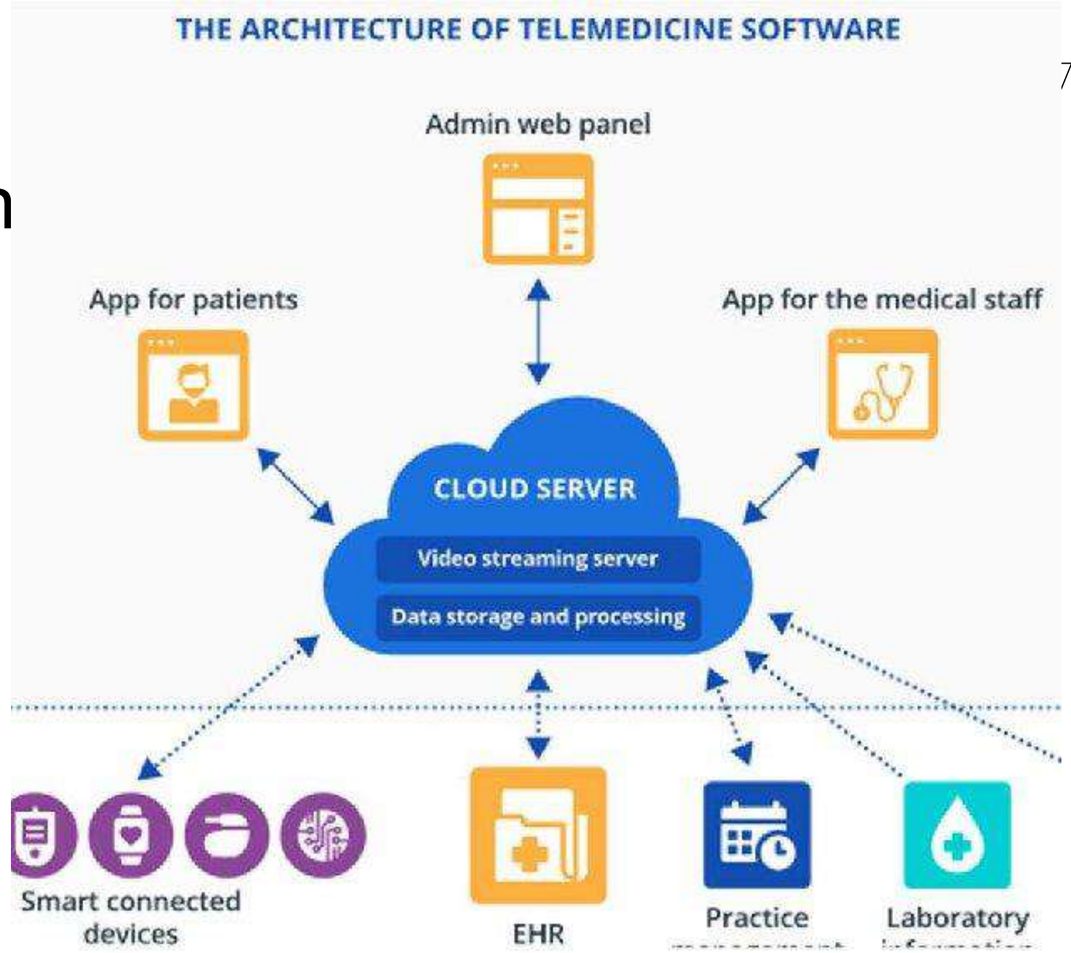
Advanced Bed and Floor Alarm for Elderly Monitoring

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Cloud Computing & Data Man

Centralized storage, backup, and access of telemedicine records and consultations.
Disaster recovery solutions; guarantees uptime and data integrity.
Scalable to match demand spikes (e.g., during pandemics).



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Security Protocols & Patient Privacy

Encryption: End-to-end for data in transit & at rest.
Access Control: Role-based permissions, authentication (ideally multi-factor).
Audit Logs & Monitoring: Detects suspicious activity, ensures regulatory compliance.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

What is Cryptography?

Cryptography is the practice of protecting information through the use of coded algorithms, hashes, and signatures. The information can be at rest such as a file on a hard drive. The information can also be in transit such as electronic communication exchanged between two or more parties.

Cryptography has four primary goals:
- Confidentiality – Makes information available to only authorized users.
- Data Integrity – Ensures that information has not been manipulated.
- Authentication – Confirms the authenticity of information or the identity of a user.
- Nonrepudiation – Prevents a user from denying prior commitments or actions.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Encryption and decryption

Encryption is the process of converting plaintext readable data to an unreadable form, known as ciphertext, to protect it. The formula used to encrypt the data, known as an encryption algorithm , must be almost impossible (using current and anticipated technology) to reverse without knowledge of the inputs to the algorithm. These inputs can include an encryption key and other random and determined data.

The process of turning ciphertext back into plaintext is called decryption. Decryption algorithms typically require an encryption key and can require other inputs, such as initialization vectors (IVs) and additional authenticated data (AAD). AAD is nonsecret data that is provided to encryption and decryption operations to add provide an additional integrity and authenticity check on the encrypted data.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Encryption algorithm

A procedure or ordered set of instructions that specifies precisely how plaintext data is transformed into encrypted data or ciphertext. The input to an encryption algorithms includes the plaintext data and a encryption key. The output includes the ciphertext.

For example, AWS Key Management Service (AWS KMS) uses the Advanced Encryption Standard (AES) symmetric algorithm in Galois/Counter Mode (GCM), known as AES-GCM.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Symmetric Algorithms

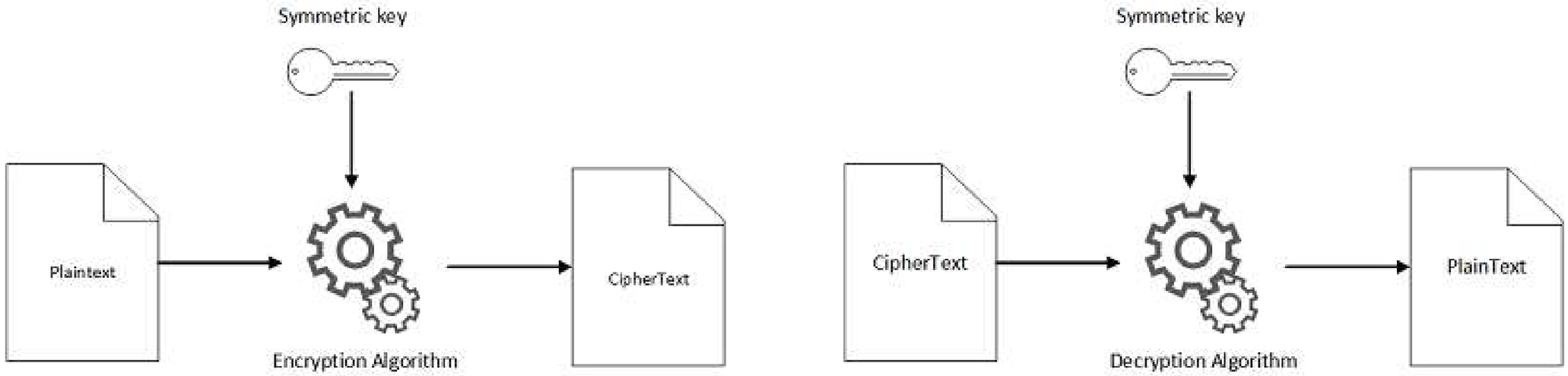
An encryption scheme is called symmetric if it uses the same key to both encrypt and decrypt plaintext.

- AES – Advanced Encryption Standard (AES) with 128-, 192-, or 256-bit keys. AES is often combined with Galois/Counter Mode (GCM) and known as AES-GCM.
- Triple DES – Triple DES (3DES) uses three 56-bit keys. The scheme works on a block of data by splitting it in two and iteratively applying arbitrary round functions derived from an initial function. Triple DES uses 48 rounds to encrypt a block of data.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Symmetric Algorithms



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Asymmetric Algorithms

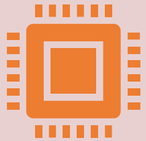
An encryption scheme is called asymmetric if it uses one key to encrypt and a different, but mathematically related, key to decrypt. Therefore, one key can be distributed publicly while the related key is kept secret and secure. Together the keys are referred to as a key pair.
The key that's publicly distributed is called the public key and the key that's kept secret is called the private key.

Public and private key

Public and private keys are used to protect data in an asymmetric encryption scheme.
Public and private keys are algorithmically generated in tandem: the public key is distributed to multiple trusted entities, and one of its paired private keys is distributed to a single entity. This way, a message can be authenticated because the public key signature proves that a trusted entity encrypted and sent it. The message contents can also be secured so that only a private key holder can decrypt it.

Public key infrastructure

Public key infrastructure (PKI) is a system of hardware, software, people, policies, documents, and procedures. It includes the creation, issuance, management, distribution, usage, storage, and revocation of digital certificates. These certificates are then used to authenticate the identities of various actors across the data transfer process.



They also assure that the data being moved between these actors is secured and encrypted in a way that both parties can decrypt. This way, information is only being sent to and received from known and trusted sources, and both parties are assured of the information's integrity.

PKI trust is established by a certificate authority (CA), which is an organization or governing body that can issue certificates and verify the identity of the certificate requestor.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Certificate authority

A trusted third party that issues (and, if necessary, revokes) digital certificates. The most common type of certificate is based on the ISO X.509 standard. An X.509 certificate affirms the identity of the certificate subject and binds that identity to a public key. The subject can be a user, an application, a computer, or other device.

The CA signs a certificate by hashing (usually by SHA256) the contents and then encrypting the hash with the private key related to the public key in the certificate. A client application such as a web browser that needs to affirm the identity of a subject uses the public key to decrypt the certificate signature.

It then hashes the certificate contents and compares the hashed value to the decrypted signature to determine whether they match.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Cryptographic Failures

This includes both misapplied cryptography and not applied cryptography and applies to data at rest and data in transit. The practices that can create threats to private, sensitive, and confidential data, include, among others, the following:
Data in transit are transmitted in the clear, meaning unencrypted, beyond a local network.
Older, weak, or deprecated encryption algorithms in use by older application software or as defaults in older equipment (HINT: use Blowfish, AES, RSA)
Encryption is not included in data storage or transmission procedures and policies.
User account passwords are in use as encryption keys.
Deprecated or weak hashing algorithms in use, such as MD5 or SHA1, or unencrypted hashing functions are in use when encryption is required (HINT: use SHA512)

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

What is process of Hashing?

Hashing turns something (usually a key or a password) into a (usually fixed length) string of characters. For example, your hashing algorithm might always produce a string that is 8 bytes long. As with encryption you transform something intelligible into something unintelligible. You cannot *decrypt* something that you have hashed. Another difference is that hashing doesn't require a key.

Uses: One use of hashing is if you want to send someone a file. But you are afraid that someone else might intercept the file and change it. So a way that the recipient can make sure that it is the right file is if you post the hash value publicly. That way the recipient can compute the hash value of the file received and check that it matches the hash value.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Applications:
One-way hash functions

Public Key Algorithms

- Password Logins
- Encryption Key Management
- Digital Signatures

Integrity Checking

- Virus and Malware Scanning

Authentication

- Secure Web Connections
- (PGP, SSL, SSH, S/MIME)

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Cryptography Hash functions

Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called message digest or simply hash values

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Additional remarks: Regulatory & Legal Compliance

Must meet national and international standards: GDPR (EU), HIPAA (US), HITECH.
Consent management: Patients must explicitly agree to telemedicine interactions and data use.
Data protection: Secure handling, storage, transfer, and deletion as required.
Cross-border requirements: Licensure, jurisdiction, data localization.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Additional remarks: Technical Support, Usability & Accessibility

24/7 help desk, troubleshooting guides.
Ongoing updates, bug fixes, software maintenance.
Platforms must be accessible to users with disabilities.
Options for low-bandwidth, multiple languages, simple interfaces.
Support/training materials for non-tech-savvy patients and staff.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Common Challenges

Infrastructure gaps in remote/low-resource areas.
Device or software compatibility issues.
Digital literacy barriers; need for patient/provider education.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Thank you!

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.