MEDICI

THE CLINICAL CODING & ANALYTICS PLATFORM

SECURITY AND SHARED RESPONSIBILITY

QUICK OVERVIEW

2021

greenlake medical

MEDICI: THE STANDARD FOR SECURE CODING AND GROUPING

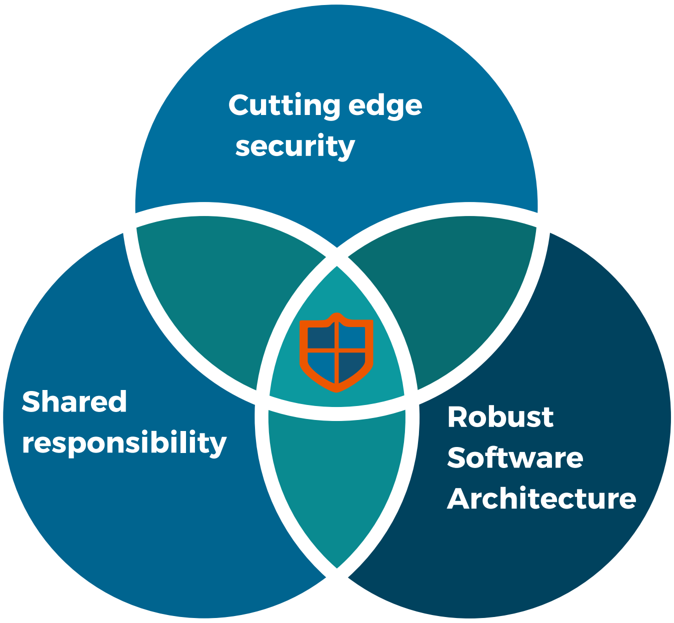
The Medici platform is at the forefront of secure coding & grouping. It seamlessly handles health data privacy, regulatory & audit requirements while ensuring rapid coding & grouping. Learn more about the system designed to help you succeed in an era of change.

SECURE MEDICAL CODING & BILLING

The Australian Privacy Act, New Zealand Privacy Act as well as the stringent HIPAA and GDPR regulations mandate strict requirements to transmit, process and store health data. At the same time, attempts to breach healthcare IT networks have been increasing globally.
Healthcare providers and insurers need systems that are built for this reality.

MEDICI NOS: SECURITY FOR THE 21ST CENTURY

The Medici NOS system dramatically improves security and compliance while enhancing the clinical coding workflow. This is achieved via a 3-factor approach.



THE THREE KEY FACTORS

Cutting edge security & data safeguards

- Data encrypted at rest and in motion (at or above 256 bit AES).
- 2-FA access control.
- Access logging.
- CIS compliant hardened containers resilient to a variety of attacks.
- Meets and exceeds AU & NZ privacy act requirements for healthcare data processing.

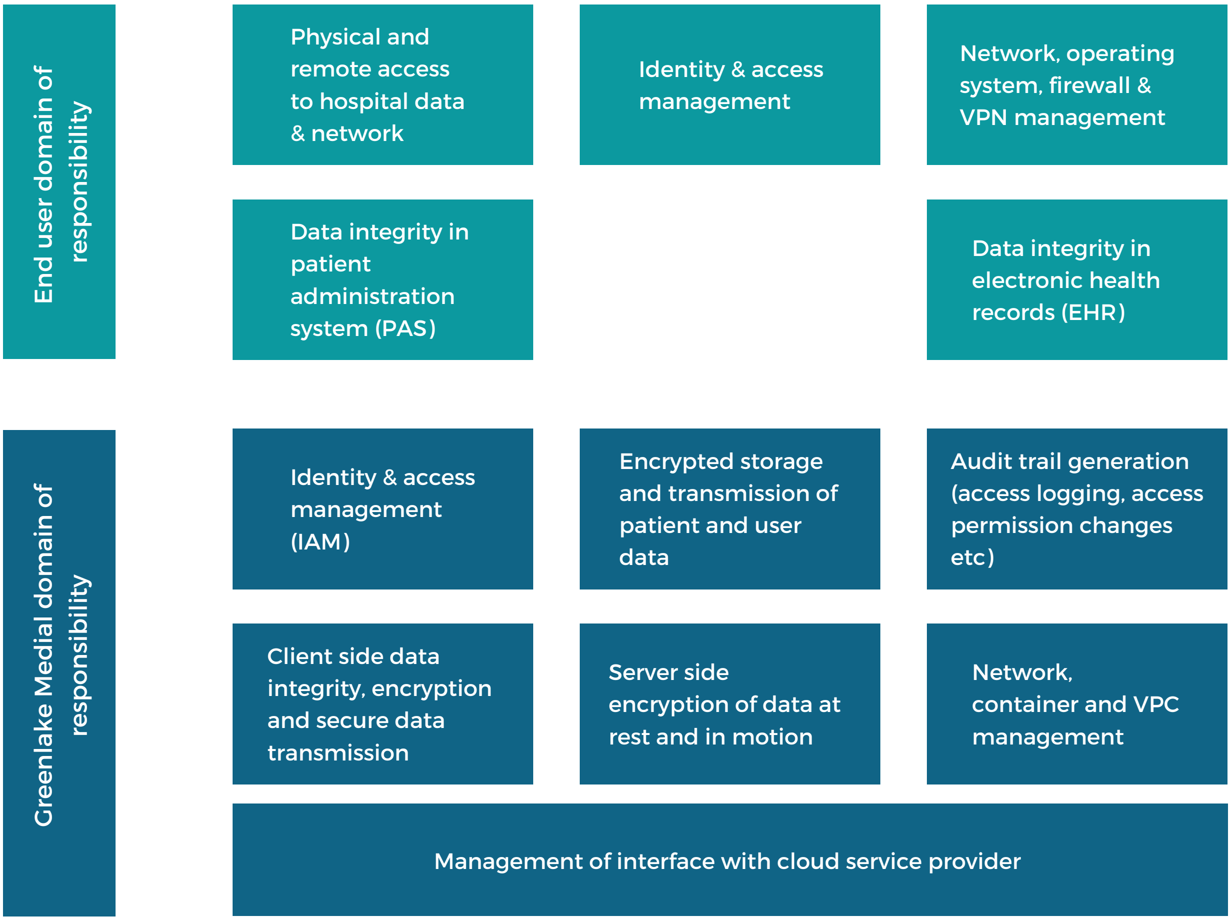
Modern, scalable and robust architecture

- No local installation - reduced attack surface (both for on-premises & cloud).
- Frequent security scans on each line of code to stay ahead of the curve.
- Streamlined permissions granting and revocation.
- Upgrade and deployment cycles with no-downtime.

Shared responsibility model

- Current best practices used across the cloud computing security industry.
- Outlines clear domains of responsibility for participants in the data processing chain

THE ON-CLOUD SHARED RESPONSIBILITY MODEL



End user domain of responsibility

Physical and remote access to hospital data & network

Identity & access management

Network, operating system, firewall & VPN management

Data integrity in patient administration system (PAS)

Data integrity in electronic health records (EHR)

Greenlake Medial domain of responsibility

Identity & access management (IAM)

Encrypted storage and transmission of patient and user data

Audit trail generation (access logging, access permission changes etc)

Client side data integrity, encryption and secure data transmission

Server side encryption of data at rest and in motion

Network, container and VPC management

Management of interface with cloud service provider

In the on-cloud model, the IT systems and administrators of the end user (hospital, health care center, insurance firm) are responsible for data and personnel access and integrity prior to the data being fed into the Medici platform.

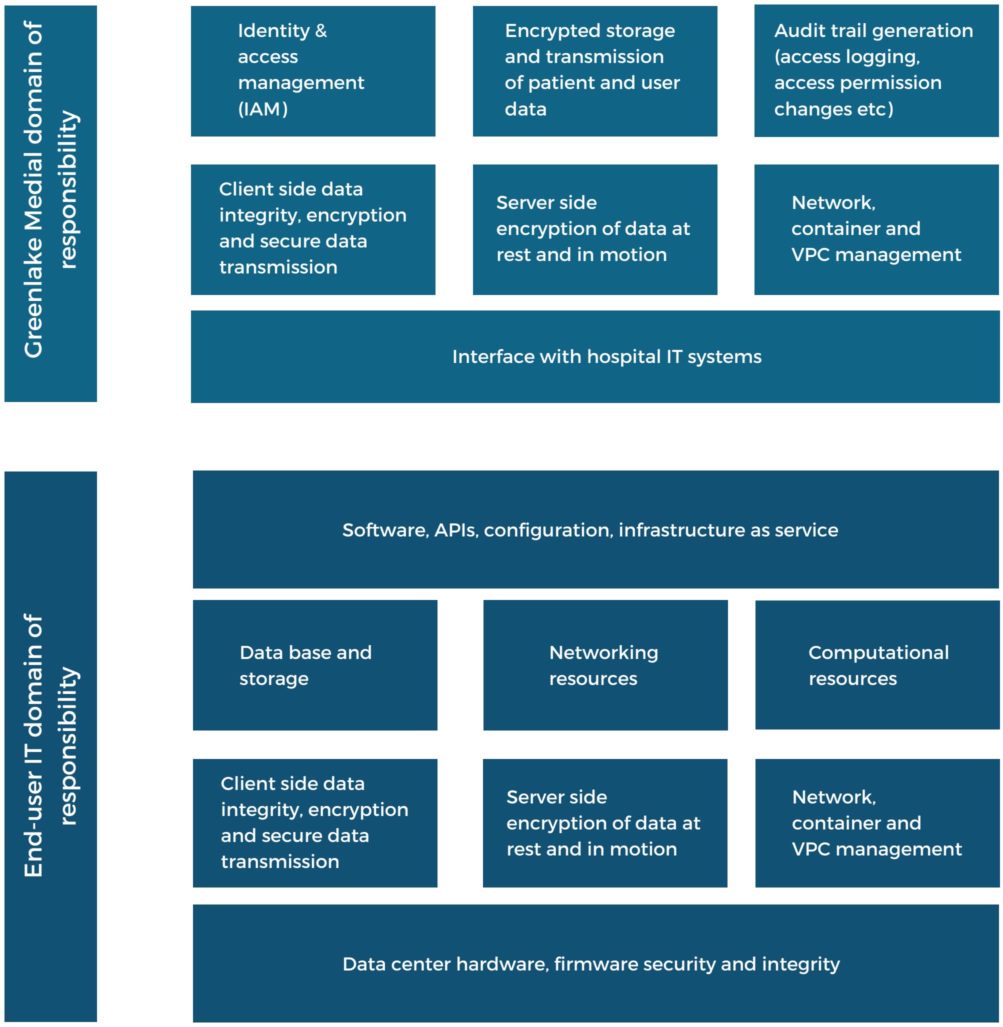
The platform is responsible for the handling of data in the cloud by interfacing with cloud providers via APIs and security mechanisms in a seamless manner.

Thus the hospital IT staff can provide their coders access to the Medici system with minimum complexity - while ensuring that key requirements will be met (in an easy to audit manner) owing to the shared responsibility model.

The end to end security mechanisms ensure that even the cloud hosting/service provider can not have access to the patient notes and data being stored in the cloud. The architecture allows changes to be rolled out without disrupting operations.

Thus patches, upgrades and new machine learning algorithms can be rolled out without affecting the service or creating any down time. Further, any new codes, modifications to code lists or changes in coding conventions can be rolled out across all medical facilities almost immediately upon acceptance - enabling rapid fixes, ensuring regulatory compliance and minimizing the impact of changes.

THE ON-PREMISES SHARED RESPONSIBILITY MODEL



Greenlake Medial domain of responsibility

Identity & access management (IAM)

Encrypted storage and transmission of patient and user data

Audit trail generation (access logging, access permission changes etc)

Client side data integrity, encryption and secure data transmission

Server side encryption of data at rest and in motion

Network, container and VPC management

Interface with hospital IT systems

End-user IT domain of responsibility

Software, APIs, configuration, infrastructure as service

Data base and storage

Networking resources

Computational resources

Client side data integrity, encryption and secure data transmission

Server side encryption of data at rest and in motion

Network, container and VPC management

Data center hardware, firmware security and integrity

In the on-premises model, the IT systems and administrators of the end-user (hospital, health care center, insurance firm) are responsible for not only the end-user items mentioned in the in-cloud case but **in addition** are also responsible for the functions that are otherwise performed by the cloud/IT hosting provider (AWS, Azure, GCP).

In this configuration the end-user IT is responsible for the safety and security of the infrastructure for health data storage , processing and audit regulations as the data remains inside the end-user IT network. This setup and management of Medici even in this case is greatly simplified owing to the use of standard containerization technologies. These architectures have been tested by leading enterprises across the world in highly demanding scenarios.

Hence for mandatory on-premises requirements, the on-site option provides a standardized secure setup of the Medici system inside your organization.

SECURITY BENEFITS AT A GLANCE

MANAGERS

Benefit from best in class data security compliance & access management, clear auditable coding and more effective coding.

- State of the art secure platform with data encryption at rest and during transit
- Meets and exceeds the requirements of AU & NZ privacy acts.
- Clear access logs and permission audit trails.

CODERS

Hassle free. Coders can focus their time on coding & grouping. Security processes are handled seamlessly.

- No installations or updates required on coder's computers.
- Access to required digital records via a single platform.
- 2-factor authentication and other best in class user-facing security workflow.

IT ADMINS

IT staff benefit from easy setup and deployment in the cloud or on-site. The modern, robust and secure architecture, and streamlined encryption and auditing ensure that your IT staff can expect a secure, minimum fuss deployment and scale up process.

- Best in class security embedded at the core.
- No downtime during upgrades/ updates & security patches.
- Frequent vulnerability scan of entire code base.
- Compatible with Amazon (AWS), Azure and Google Cloud.
- Supports deployment entirely within on-premises IT infrastructure.
- Protection from OWASP Top-10 threats

GET STARTED

Contact us to learn how Medici can accelerate your organisation's coding and grouping while keeping your data secure. Start measuring benefits within weeks rather than months.

Greenlake Medical Pty Ltd
Suite 108, Level 23,
Collins Square Tower 5,
727 Collins St, Melbourne VIC 3008
e: sales@greenlakemedical.ai