Date: August, 2023

randtronics

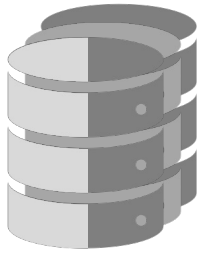
Protecting Health Records

Case Study: Enterprise encryption for GDPR & HIPAA Compliance

The Challenge: Complex environment with many participants and multiple systems

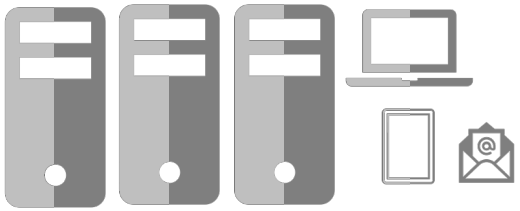
For many hospitals, protecting sensitive patient data is a particular challenge:

- Sensitive data is stored on multiple IT systems
- Multiple IT platforms to be protected
- Budget: so many things clinical things to spend on, so non-clinical IT investments heavily scrutinized
- Clinicians adverse to security protocols that might interfere with their care provision
- Data shared with nurses, therapists, doctors: on-staff, visiting specialists and primary care providers
- Staff: thinly stretched IT staff and may lack the bandwidth and/or skills to make code changes when implementing cyber-security provisions
- Regulated environment with a mandatory requirement to demonstrate protection of patient-related data



Sensitive data stored in multiple databases

Sensitive data stored on multiple environments



Multiple Clinical Systems: Very few hospitals have a single solution:

- Electronic Health Records
- Clinical Decision Support
- Pharmacy/ Prescribing
- Pathology
- Patient Billing
- Clinical Scheduling

Patient related data needs to be protected across multiple databases, servers, end devices and in emails

Solution: Centralized platform for protecting sensitive data on databases, servers and end-devices

Centralized, policy-driven system that makes it easy to implement and manage cryptography protection across complex environments:

1) Transparent Data Encryption (TDE) for any/all databases, servers, files, folders and laptops
2) Masking and Tokenization & Enterprise Key Management
3) Protection of content shared across insecure media: email, USB-drive, public cloud storage

Enterprise, encryption-management platform

Mission: making easy for organizations to encrypt ‘everything’

Protecting patient data in over 50 hospitals

- Randtronics DPM is protecting patient data in over 50 hospitals across North America and Asia
- Includes:
  - USA specialty hospitals: transparent data encryption of electronic health record databases and servers
  - Large Asia Telco: providing encryption-as-a-service database and server protection to multiple hospitals using Randtronics software

Example: TDE protection of EHR

- EHR system, MS-SQL database backend, running on Windows servers
- HIPPA and GDPR compliance requirement to encrypt data, protect keys, restrict access and provide role separation and auditability
- No scope to make code changes
  - Packaged software from large vendor
  - Thinly stretched IT staff with limited bandwidth and lacking skills and experience to implement and support local code changes

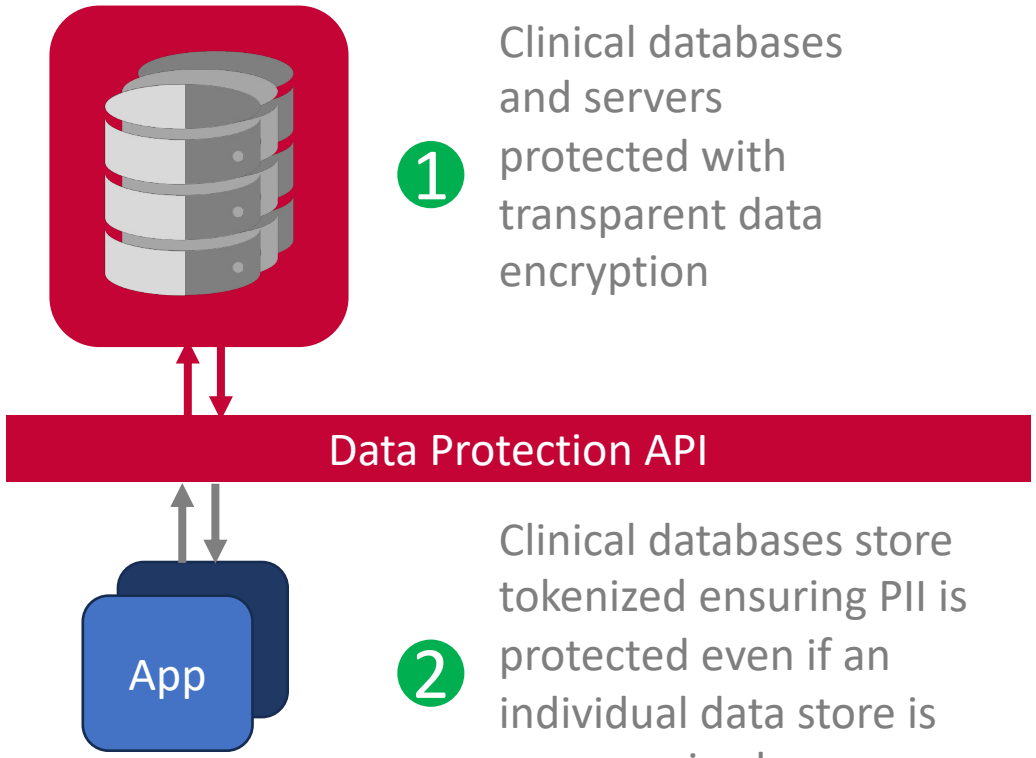
Solution – Server Level TDE

Encrypt **DB server, App Server & File Server** protect DB plus Log files, reports, passwords, certificates, config files, key files, etc.

Encrypt **Folders** on end devices containing cached copies of data and materials shared with patients and other care providers

Example: Multi-layered data protection

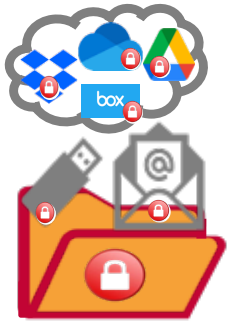
- Health organizations seeking to implemented standardized data protection
  - Protect all clinical IT systems including legacy systems requiring no-code change protection
  - Providing options for multi-layer data protection – field-level data protection via API plus Transparent Data Encryption
  - Enabling BYOD data protection
  - Providing standard methods for data sanitization for analytics, reporting and archiving
  - Centralized, auditable policy-driven data protection



Example: Secure sharing of reports

- Test results, referrals and reports need to shared with patients, primary care providers, specialists
- Overt demonstration of protection helpful in migrating clinicians off fax
- Need a solution that ensures that only the intended recipient can read
- Need a solution that is very straightforward and can be used with anyone

Solution – DPM easy2Go



DPM easy2Go

- Point and Click encryption
- Protect with Password or Digital Certificate
- Reader edition version available for free-download
- Strong assurance that contents can only be read by intended audience
  - Send password via SMS
  - Inherent with use of Digital Certificate

Example: Sanitizing shared or archived records

- Health organizations wishing to:
  a) share aggregate patient information for analytics, or
  b) Maintain long term records free from identifiable patient details
- Need a means of parsing Text files and CSV files to remove/mask or redact patient identifying information

Solution – File Tokenization

- Point and Click encryption
- Protect with Password or Digital Certificate
- Reader edition version available for free-download
- Strong assurance that contents can only be read by intended audience
  - Send password via SMS
  - Inherent with use of Digital Certificate

Randtronics LLC

Milpitas CA 95035 United States
+1 (650) 241 2671
enquiry@randtronics.com

Randtronics Pty Limited

S1.1, Level 1, Building A 64 Talavera Road
North Ryde, NSW 2113 Australia
+61 418 226 234

Thank you for your time

email: bob.adhar@randtronics.com

Cell: +614 18 226 234 or +1 650 241 2671