Fortifying the Future:
Data Privacy & Security in Behavioral Health AI

Rony Gadiwalla
CIO
GRAND Mental Health

Raz Karmi
CISO
Eleos

Nisheeta Setlur
VP, Client Success
Eleos

eleos

Housekeeping

- Slides & recording will be distributed
- Post questions using the Q&A function at any time. We'll follow up with any unanswered questions.
- Tell us how we did in the post-webinar survey

eleos

Our Speakers

Rony Gadiwalla
CIO
GRAND Mental Health

Raz Karmi
CISO
Eleos

Nisheeta Setlur
VP, Client Success
Eleos

eleos

Our Agenda

1. Where AI regulations stand today
2. Discussion!
3. How Eleos approaches security & privacy
4. Q & A

eleos

Key Terms

Traditional certifications

Evaluate core security principles such as confidentiality, integrity, and access; centered around effective information security management.

Healthcare-specific

Regulations that are relevant to anyone–and anything–that collects, handles, transfers, or shares health data.

Guidelines & Frameworks

Best practices and policies that Eleos considers a priority, though they are not required by law–yet.

eleos

AI Regulatory Climate: Where We Stand

Rules & Guidelines

AI-Specific Policy & Principles

- EOs 13859-14110
- The AI Bill of Rights
- ISO 42001
- OECD Principles on AI
- UNESCO
- HHS Trustworthy AI Playbook
- ONC HT-1 Final Rule

Healthcare-Specific Regulations

- HIPAA
- HITRUST
- 21st Century Cures Act

Security-Specific Certs

- ISO (27001 & 27799)
- SOC 2

Guidelines & Frameworks

- HIA Principles
- The METRIC-framework for Assessing Data Quality for Trustworthy AI in Medicine
- The Center for Human-Compatible AI (CHAI)

eleos

AI Regulatory Climate: Where We Stand

- Executive Order 13859 on American Leadership in AI February 2019
- Executive Order 13960 on Trustworthy AI Principles December 2020
- Executive Order 13985 on Advancing Racial Equality January 2021
- HHS Trustworthy AI Playbook September 2021
- AI Bill of Rights October 2022
- Executive Order 14091 on Further Advancing Racial Equality February 2023
- ONC Introduces FAVES Principles in HTI-1 NPRM April 2023
- Executive Order 14110 on Safe, Secure, and Trustworthy AI October 2023
- HHS Data Strategy December 2023
- White House-Industry Commitments on FAVES December 2023
- OMB Memo M-24-10 on AI Governance March 2024
- HTI-1 Final Rule January 2024
- HTI-1 Requirements December 2024
- HHS AI Strategy January 2025

The CHAI 6-Stage Lifecycle for Health AI Development and Deployment

1. Define Problem & Plan
2. Design the AI System
3. Engineer the AI Solution
4. Assess
5. Pilot
6. Deploy & Monitor

eleos

AI Regulatory Climate: What's Next

New U. S. State Legislation

- 45 states introduced AI bills in 2024
- 31 states adopted new AI regs in 2024
- Colorado mile-high AI Act

Global AI Treaty

- EU, UK, and United States
- Signed September 2024
- Likely non-enforceable

eleos

Discussion Time!

eleos

How Eleos Approaches Security & Privacy

1. Get all relevant certifications and keep up with established and emerging regulations.
2. Bring on a CISO.
3. Nail the basics—and then some.
4. Never stop learning (or updating).

eleos

Our Approach

Alignment & Enforcement.

- Adopt & enforce industry best practices
- Strict access controls such as least-privelage
- Enforce data security controls through encryption, etc.

Always Choosing Ethical AI Use.

- Transparency is the best policy
- Informed consent and the option to opt-out
- Human-in-the-Loop for accuracy and reliability
- Clinical experts review & update models

Stay Informed & Vigilant.

- Regularly monitor AI regulations and guidelines updates from relevant sources
- Never stop learning

eleos

How Eleos Approaches Security & Privacy

Our Certifications

HIPAA

HIPAA is a federal law governing how healthcare organizations and their business associates handle protected health information (PHI).

SOC 2

SOC 2 certification is an independent verification that a service organization's security controls are effective over a period of time.

HITRUST

HITRUST certification builds on the foundation of the SOC 2 framework, but with a specific focus on the healthcare industry.

ISO 27001

ISO 27001 certification is essentially a stamp of approval for an organization's information security management system (ISMS).

NIST CSF

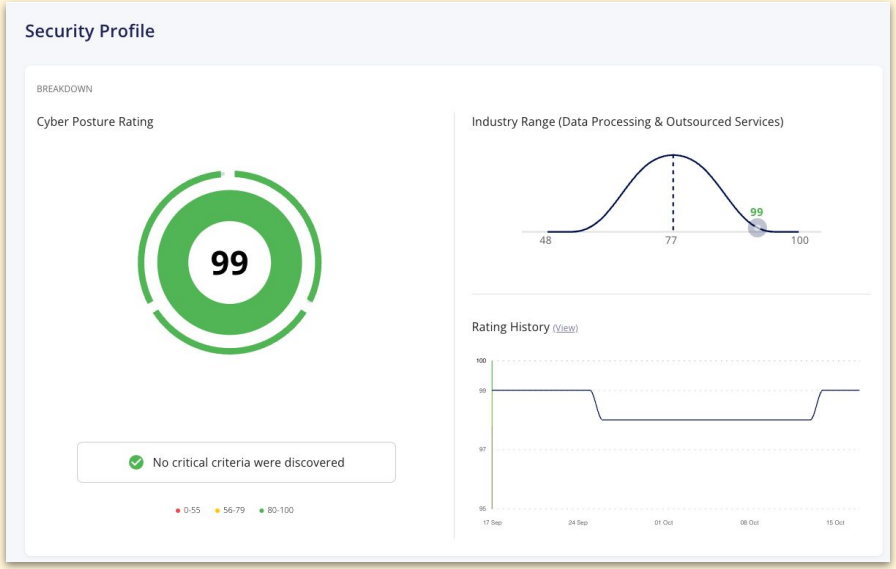
NIST CSF is an industry-standard framework for organizations of all sizes to manage their cybersecurity risks.

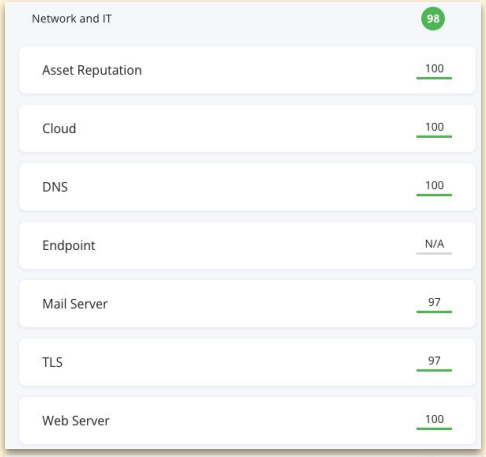
eleos

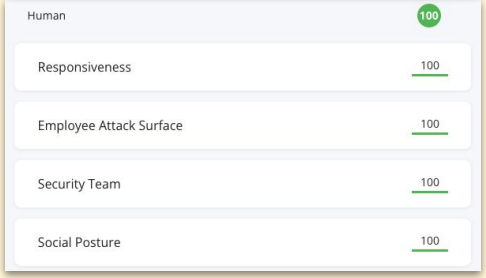
Eleos Cyber Posture Rating

Panorays

- Panorays is a top-rated Cybersecurity Risk Rating Platform
- Across three major categories of risk assessment, Eleos received “Excellent” posture ratings







eleos

How Eleos Approaches Security & Privacy

The CISO Role

- How is a CISO different from a CIO?
- What does a CISO do?
- Why does a CISO matter—especially in behavioral health?

eleos

How Eleos Approaches Security & Privacy

Beyond the Basics

- Why HIPAA, HITRUST, & SOC are just the beginning
- OWASP Top 10
  - What are the OWASP top 10?
  - Why do they matter?
- Frameworks & guidelines followed by Eleos

eleos

Beyond the Basics

How Eleos Approaches Security & Privacy

Eleos is constantly evaluating and researching best practices and implementing new policies to stay ahead of the tech curve.

eleos

Internal Secure AI System Development Policy	OWASP LLM top 10	NIST's AI Risk Management Framework
Google's Secure AI Framework (SAIF)	MITRE Atlas OWASP Top 10 for LLM Applications	MITRE Atlas
Cloud provider best practices	MIT AI Risk Repository	Center for AI safety

How Eleos Approaches Security & Privacy

Always Learning & Iterating

- How Eleos stays on top of regulatory news & changes
- Eleos' annual update policies
- Considerations for AI ethics & bias

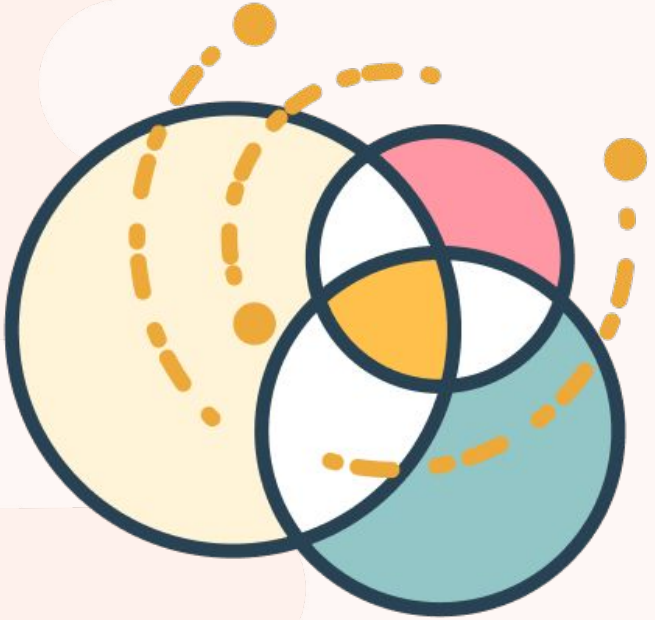
eleos

Our Responsibility & Commitment.

1. Adhere to the security and privacy standards outlined in the agreements & contracts.
2. Implement security measures to protect all data.
3. Implement security best practices through the entire AI development lifecycle.
4. Be transparent about security practices and notify the organization of any changes.
5. Ensure any and all subcontractors also comply with data protection requirements.

eleos

Q&A



eleos

Check out our CISO FAQ blog to learn more →

Thank you for attending!

eleos

Fortifying the Future: Data Privacy & Security in Behavioral Health AI

eleos

AI Regulatory Climate: Where we Stand

Regs & Frameworks

AI-specific

- EOs 13859-14110
- The AI Bill of Rights
- HHS Trustworthy AI Playbook
- ONC HT-1 Final Rule

Healthcare specific

- HIPAA
- HITRUST
- ISO (27001 & 27799)
- SOC 2

Guidelines & Frameworks

- HIA Principles
- The METRIC-framework for Assessing Data Quality for Trustworthy AI in Medicine
- The Center for Human-Compatible AI (CHAI)

Executive Order 13859 on American Leadership in AI
February 2019

Executive Order 13960 on Trustworthy AI Principles
December 2020

Executive Order 13985 on Advancing Racial Equality
January 2021

HHS Trustworthy AI Playbook
September 2021

AI Bill of Rights
October 2022

Executive Order 14091 on Further Advancing Racial Equality
February 2023

ONC Introduces FAVES Principles in HTI-1 NPRM
April 2023

Executive Order 14110 on Safe, Secure, and Trustworthy AI
October 2023

HHS Data Strategy
December 2023

White House-Industry Commitments on FAVES
December 2023

OMB Memo M-24-10 on AI Governance
March 2024

HTI-1 Final Rule
January 2024

HTI-1 Requirements
December 2024

HHS AI Strategy
January 2025

The CHAI 6-Stage Lifecycle for Health AI Development and Deployment

1 Define Problem & Plan
2 Design the AI System
3 Design the AI System
4 Assess
5 Pilot
6 Deploy & Monitor

eleos

Regulations, frameworks & best practices

Traditional certifications	Healthcare	State specific	AI	EU	In progress
Focus on core security principles such as confidentiality, integrity, and availability and centered around effective information security management	*Relevant to anyone and anything that collects, handles, transfers, or shares health data.*	*State specific regulations*	*AI specific regulations and certifications*	*applicable in the EU, has strict requirements for data privacy and consent.*	*Regulations, frameworks & best practices in progress*
SOC2 Type II	*HIPAA*	*California Consumer Privacy Act (CCPA)*	*ISO 42001*	*GDPR*	*The Coalition for Health AI (CHAI) organization*
ISO 27001	*HITECH*	*California Privacy Rights Act (CPRA)*	*Biden's Administration Executive Order*	*The EU AI Act*	*Colorado mile-high AI Act*
NIST Cybersecurity Framework	*HITRUST*	*Washington state "My Health, My Data" Act (MHMDA)*	*OECD Principles on AI*		
NIST AI Risk Management Framework	*21st Century Cures Act*		*UNESCO*		

eleos

Protecting sensitive information

- Security and privacy by design
- Strict access controls (MFA, Least privilege and Role-Based-Access)
- Data security controls (Visibility, Encryption, Anonymization, retention)
- AI Security (Implement a designated tool) Discover security gaps proactively
- Ongoing monitoring
- Ongoing risk assessment
- Ongoing AI system audits
- 3rd parties management

eleos