

# Healthcare In Crisis: How to Take Your HIPAA Security to the Next Level

 **CHOICE** CYBERSECURITY

 **GROSSMENDELSON**  
ACCOUNTING | TECHNOLOGY | WEALTH ADVISORY

# BILL WALTER



ASSESS



ADDRESS



MAINTAIN



**PARTNER**

## ABOUT BILL WALTER

Bill Walter is a partner in Gross Mendelsohn's Technology Solutions Group. He helps businesses of all types and sizes document and remediate security systems. With 23 years of experience, Bill's passion is helping organizations better use technology to operate more efficiently.

Cyber Security

Remediation

Technology Best Practices

# STEVE RUTKOVITZ



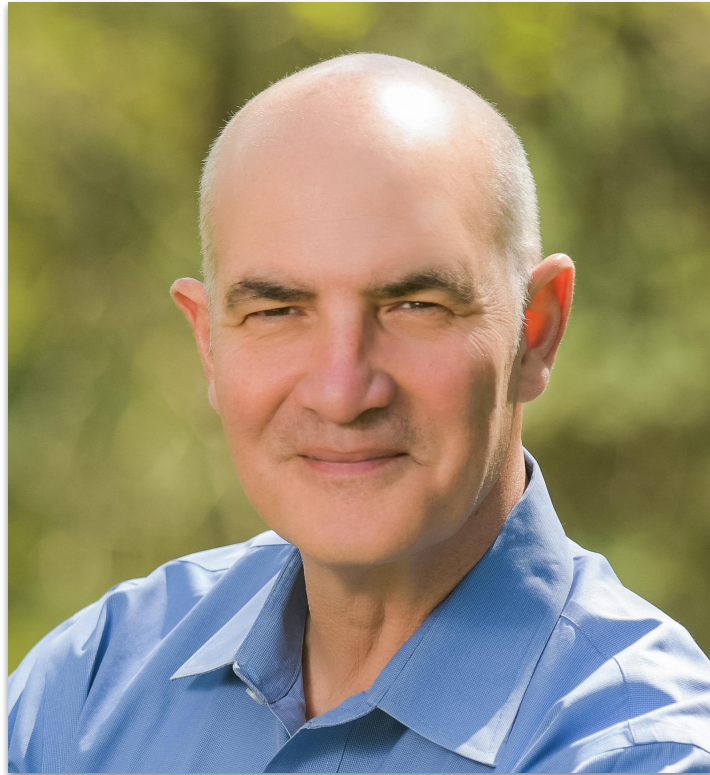
ASSESS



ADDRESS



MAINTAIN



**PRESIDENT & CEO**

## ABOUT STEVE RUTKOVITZ

For over 20 years, Steve owned and operated a very successful MSP business. With a clear understanding of the market's needs, he developed an innovative security and compliance business process to meet HIPAA, NIST and CRISP compliance.

Security and Compliance

Risk Assessments

Education

Audit Management





# Security & Compliance

## Security

- The state of being free from danger or threat

## Compliance

- The act of obeying an order, rule or request

# Industry Changes

Telemedicine



Cloud

EMR  
Phones  
Email  
Images



IOT

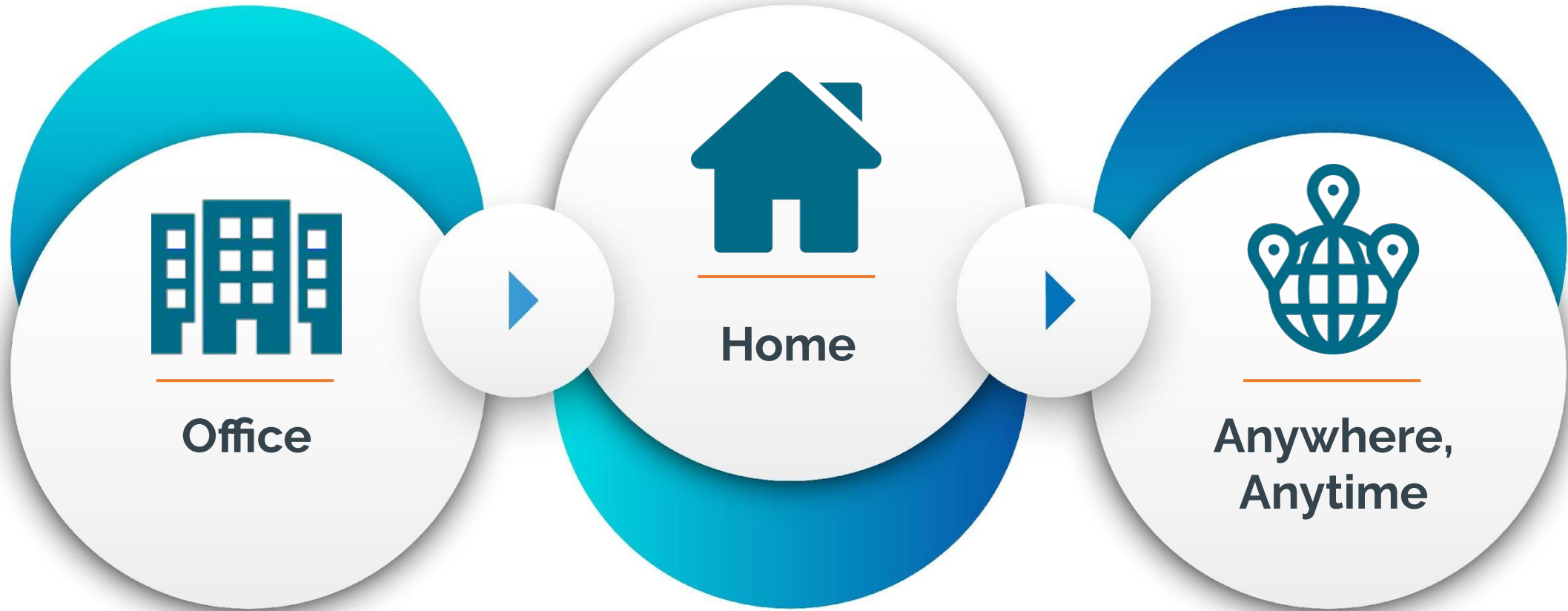
Medical Devices  
Wearables



Mobile



# The New Normal



# SECURITY

- Unique Total Risk
- Reactive to Proactive
- The Right Layers of Defense



# Cyber Threats



## TOP CYBER THREATS

1

Ransomware

2

Malware

3

Phishing Attacks

4

Brute Force Attacks

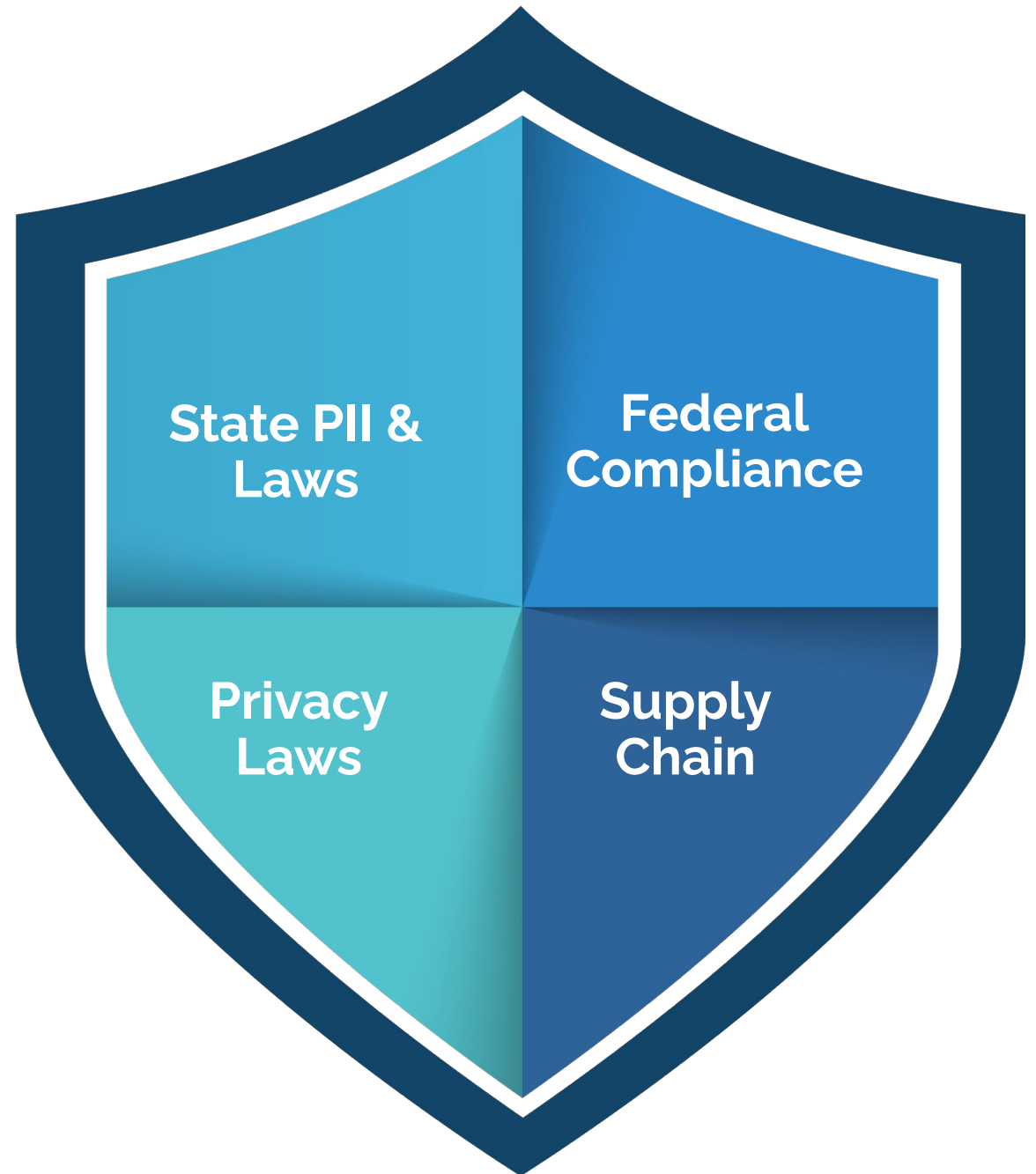
5

Insider Threats



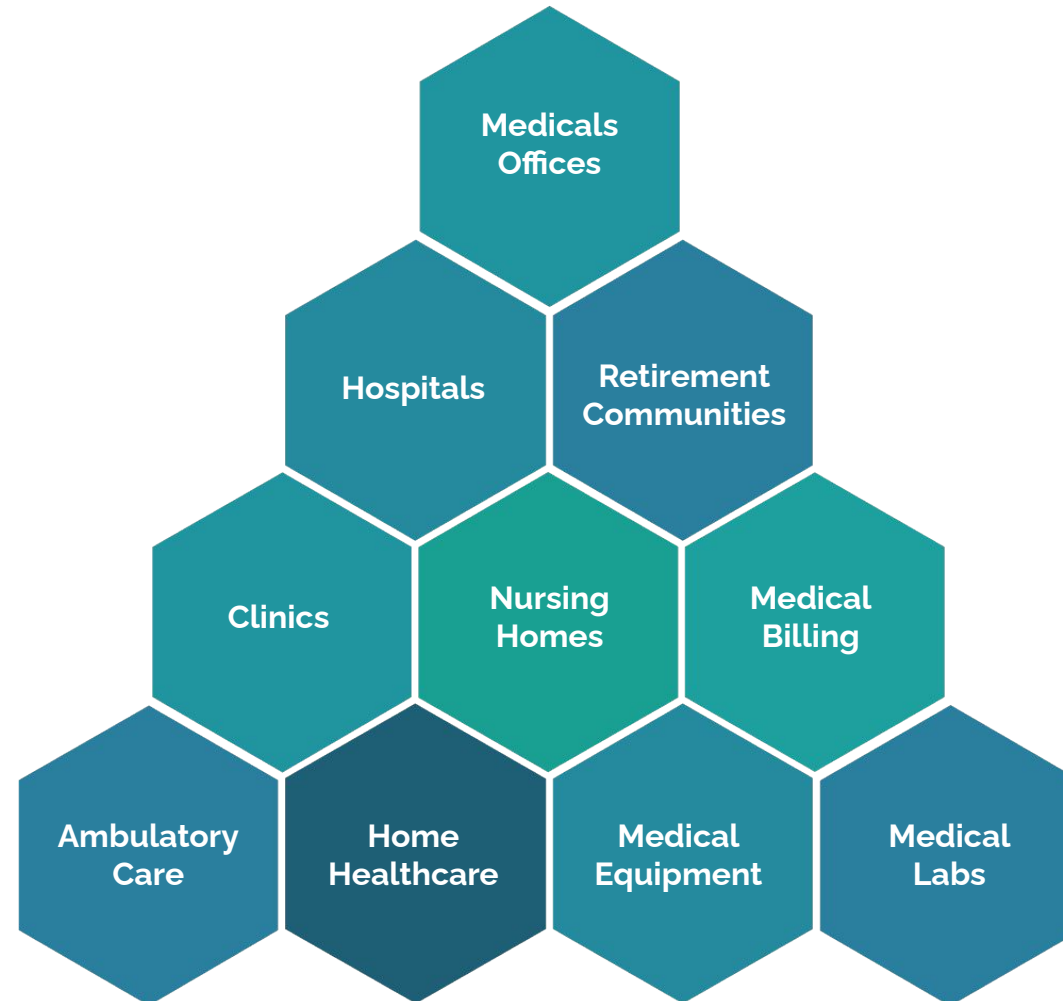
# Compliance & Best Practices

- HIPAA
- NIST
- PCI



# Healthcare

- Healthcare accounts for **17.5%** of gross domestic product
- Americans spend about **\$9,523 per person** on healthcare per year
- Total healthcare employment in 2015: **2.4 million workers**



# Healthcare Industry

---

- 1 Covered Entity (CE)**
- Health plans, healthcare clearinghouses and healthcare providers

- 2 Business Associate (BA)**
- Person or entity that works with PHI on behalf of a CE (medical billing)

- 3 Personally Identifiable Information (PII)**
- Data to identify a specific person

- 4 Electronic Protected Health Info (ePHI)**
- Protected health information stored electronically

- 5 Electronic Medical Records (EMR)**
- Digital version of a patient's medical records

- 6 Electronic Health Record (EHR)**
- Digital version of a patient's overall health

# Personal Health Information

---



Social Security Numbers

Medical Health Records

Dates of Birth

Patient Information

Medical Insurance Information

# Penalties

**\$50,000 per violation**

- 1,000 records = **\$50M**
- Capped at **\$1.5M** for identical violations during a calendar year
- By patient record
- **Safe harbor rules**



# Penalties

Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Partners HealthCare System, Inc.	MA	Healthcare Provider	2450	02/05/2018	Hacking/IT Incident	Desktop Computer
	City of Detroit	MI	Healthcare Provider	544	02/05/2018	Loss	Other Portable Electronic Device
	Eastern Maine Medical Center	ME	Healthcare Provider	660	02/02/2018	Theft	Other Portable Electronic Device
	Forrest General Hospital	MS	Healthcare Provider	1670	02/01/2018	Hacking/IT Incident	Email
	Steven Yang, D.D.S., INC.	CA	Healthcare Provider	3202	01/26/2018	Theft	Laptop
	Decatur County General Hospital	TN	Healthcare Provider	24000	01/26/2018	Hacking/IT Incident	Network Server
	Rocky Mountain Women's Health Center, Inc.	UT	Healthcare Provider	1166	01/25/2018	Improper Disposal	Paper/Films
	Zachary E. Adkins, DDS	NM	Healthcare Provider	3677	01/25/2018	Theft	Other Portable Electronic Device
	Central States Southeast and Southwest Areas Health and Welfare Fund	IL	Health Plan	634	01/23/2018	Unauthorized Access/Disclosure	Paper/Films
	RGH Enterprises, Inc.	OH	Healthcare Provider	4586	01/22/2018	Unauthorized Access/Disclosure	Paper/Films
	Robert Smith DMD, PC	TN	Healthcare Provider	1500	01/22/2018	Hacking/IT Incident	Network Server
	Westminster Ingleside King Farm Presbyterian Retirement Communities, Inc.	MD	Healthcare Provider	5228	01/19/2018	Hacking/IT Incident	Desktop Computer, Network Server
	The Pediatric Endocrinology and Diabetes Specialists	NV	Healthcare Provider	1021	01/18/2018	Hacking/IT Incident	Desktop Computer, Electronic Medical Record, Laptop
	Gillette Medical Imaging	WY	Healthcare Provider	4476	01/18/2018	Unauthorized Access/Disclosure	Paper/Films

# Drivers

---

---

## Meaningful Use

---

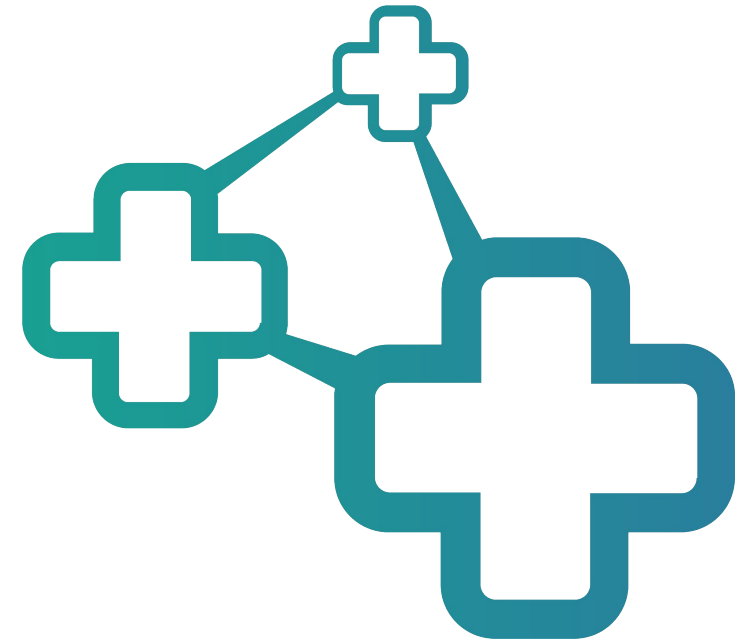
### MIPS: 25% Risk Assessment - HIPAA

\$30,000 per year in Medicare and/or 100 Medicare patients per year

---

### OCR/HHS

Risk Assessment form needs to be turned in annually



# HIPAA Components

---

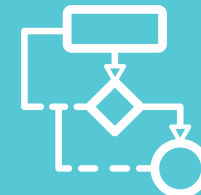
Three Components



**Administrative  
Safeguards**



**Technical  
Safeguards**



**Physical  
Safeguards**



# Technical Safegaurds

---



# Our Assessment Process

---



**ASSESS**



**ADDRESS**



**MAINTAIN**



# RISK ASSESSMENTS

---

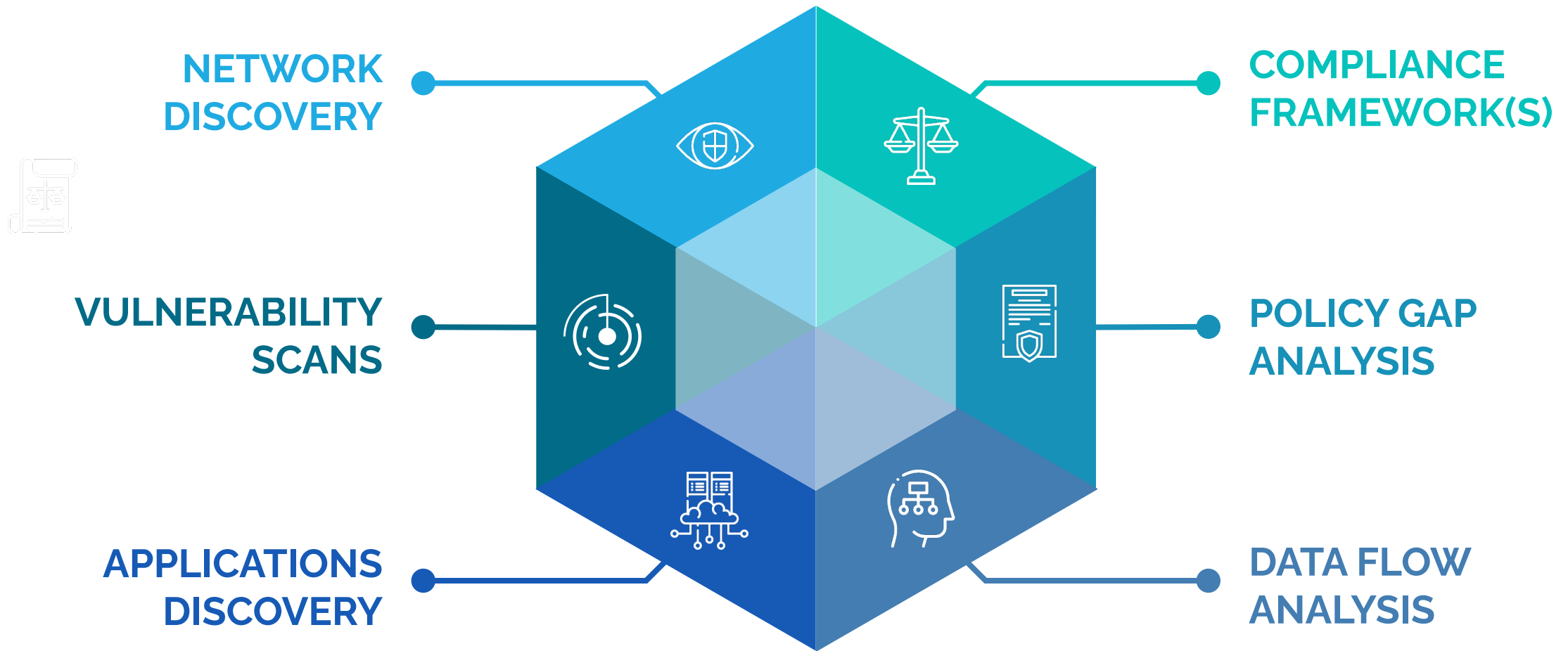
- Build a Baseline
- Uncover Gaps and Risks
- Expose Vulnerabilities
- Analyze Layers of Defense
- Identify Sensitive Data
- Missing Controls and Policies



**ASSESS**

---

# Risk Assessment Components



# PII Scan Results and Data Auditing

**TOTAL LIABILITY: \$10,043,391**

**35,000**

Medical Records

**9,936**

Credit Cards

**14,451**

Social Security  
Numbers

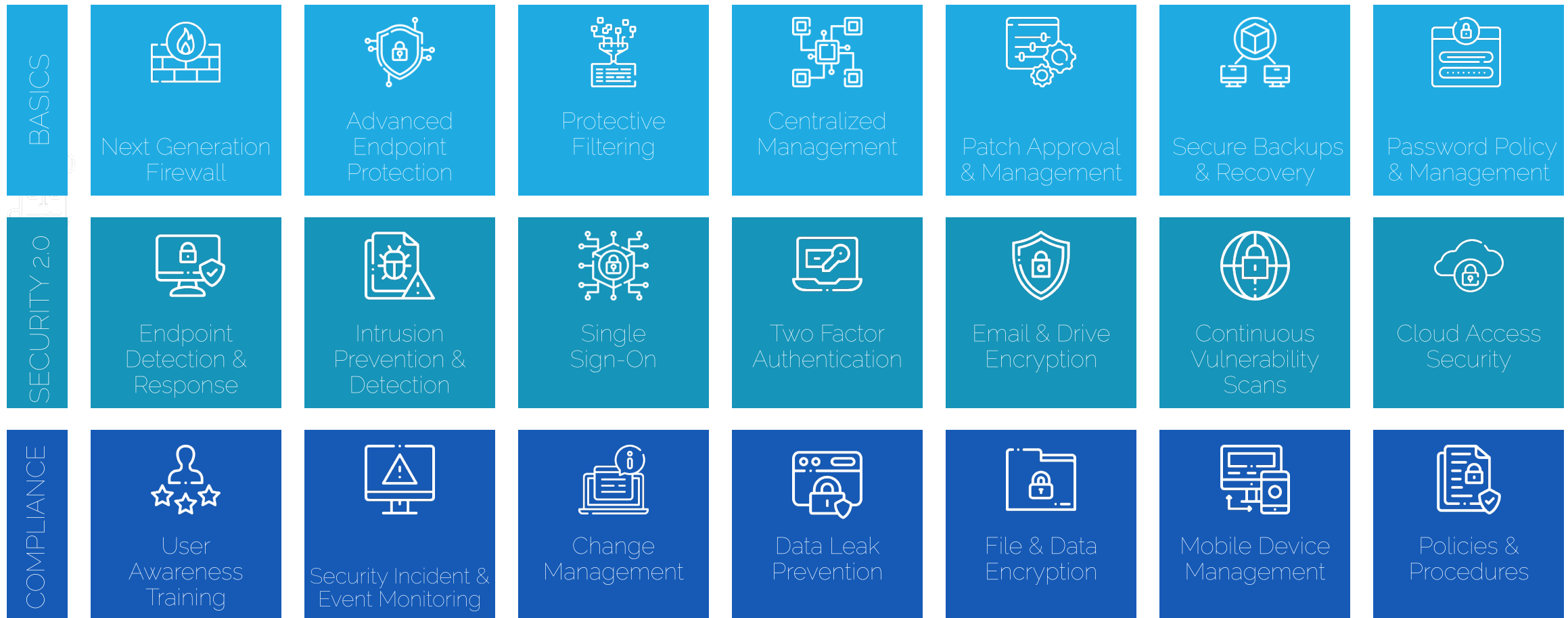
**2,746**

Dates of Birth

# HIPAA Policies & Procedures

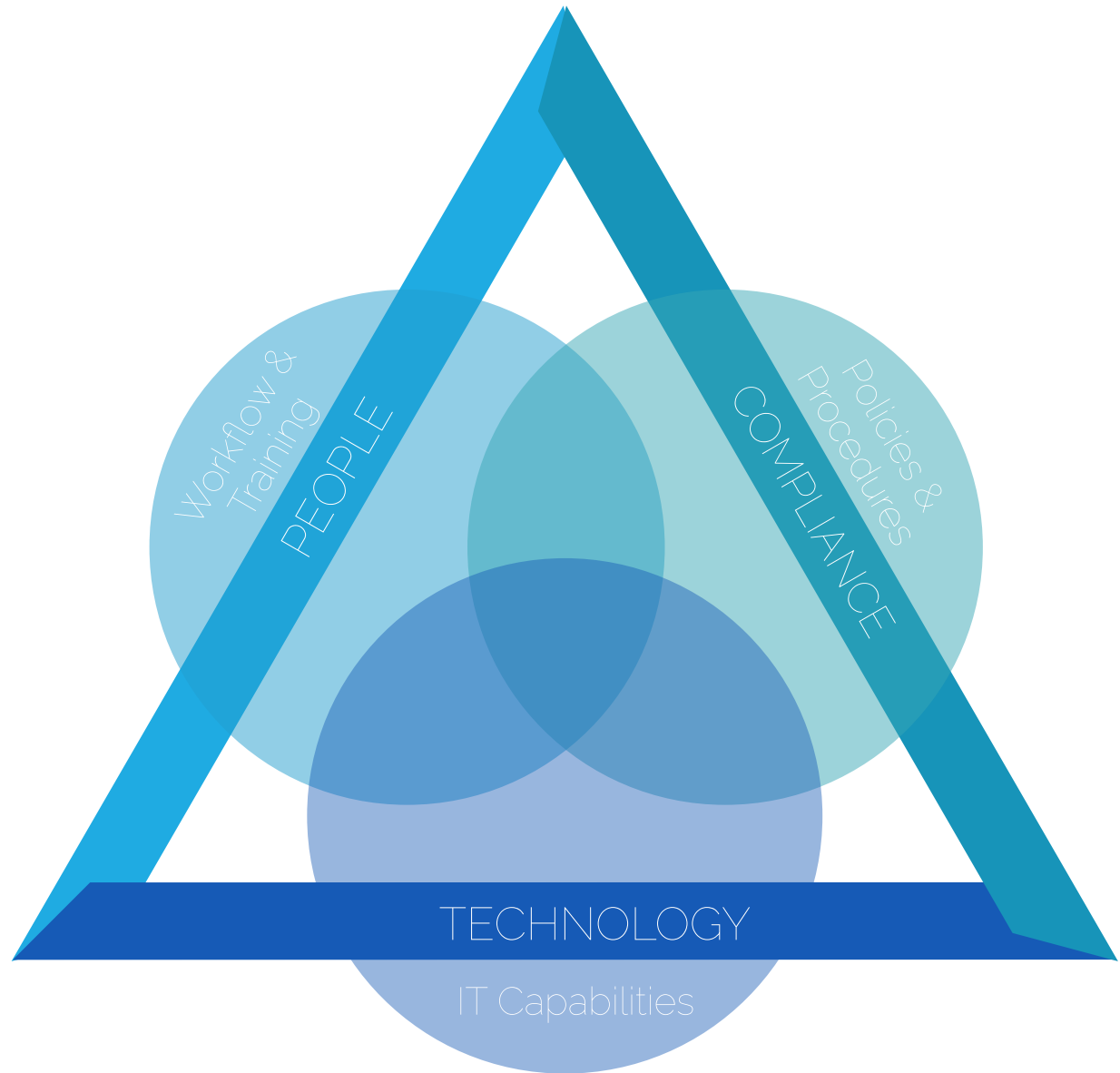
Personally Sensitive Data Definition	Monitoring & Logging Operations	Access Controls & Logging	Organizational Policy & Process Documentation	Facility Management	Protection from Malicious Code
IT Asset Physical Security	Transmission Security	Uses & Disclosure of PHI with a Valid Authorization	Notice of Privacy Practices	Individual Rights to Uses & Disclosure of PII	Encryption & Decryption
Disclosure Authorization	Physical & Environmental Security	Minimum Necessary & Limited Data Set of PHI	Amendment of PHI	Uses & Disclosure of ePHI General Rules	Incident Response & Disaster Recovery
HIPAA Privacy & Security Awareness Training	Contingency Plan	Business Associate Agreements	Individual Rights to PHI	Designating a HIPAA Privacy & Security Official	Social Media Policy
Complaints and Prevention of Retaliatory Acts	Sanctions	Risk Analysis & Management	HIPAA Terms & Definitions	Password Management	Mobile Device & Teleworking

# The Stack of Security Layers



# TOTAL RISK ALIGNMENT

---





# Choice Compliance Journey





# CHOICE CYBERSECURITY

Independent risk assessment

Works with your existing  
Managed Services Provider (MSP) or IT staff

HIPAA experience with numerous medical specialties

Complete audit readiness solutions to meet and maintain  
HIPAA compliance

Approved vendor for the Maryland Cybersecurity 50% Tax Credit

# Team of Experts



# HIT THE GROUND RUNNING

We help you MEET and MAINTAIN compliance through our all-in-one *Continuous Compliance Services*.



# Q&A



**CHOICE** CYBERSECURITY



**GROSSMENDELSONN**

ACCOUNTING | TECHNOLOGY | WEALTH ADVISORY



# CHOICE CYBERSECURITY

@ [steve@choicecybersecurity.com](mailto:steve@choicecybersecurity.com)

 [www.choicecybersecurity.com](http://www.choicecybersecurity.com)

 410.205.4980

 10065 Red Run Blvd, Suite 120  
Owings Mills, MD 21117




## GROSSMENDELSON

ACCOUNTING | TECHNOLOGY | WEALTH ADVISORY

@ [wwalter@gma-cpa.com](mailto:wwalter@gma-cpa.com)

 [www.gma-cpa.com](http://www.gma-cpa.com)

 410.685.5512

 1801 Porter Street, Suite 500  
Baltimore, MD 21230