CLEARDATA®

Healthcare's Cybersecurity

MDR Buyer's Guide

A **ClearDATA** Resource

HEALTHCARE CYBERSECURITY

Your MDR Buyers Guide

Why Read this Guide?

✓ Understand Your MDR Needs

✓ Learn Ideal Attributes of an MDR Partner

✓ Find Out How to Evaluate MDR Vendors

The healthcare sector remains a prime target for threat actors, plagued by outdated technologies and a high susceptibility to disruptions that can jeopardize access to healthcare. The average cost of a healthcare breach has seen a 10.6% decrease, now sitting at USD 9.77 million. Despite this positive trend, healthcare continues to hold the unfortunate title of the costliest industry for breaches—a distinction it has maintained since 2011.

So what's the answer? A Managed Detection & Response (MDR) solution that is both defensive and offensive to protect against healthcare's greatest threats. Unlike traditional security measures that react to threats after they occur, the best MDR solutions enable healthcare organizations to proactively identify exposure in the attack surface and rapidly mitigate risks before they can be exploited.

CONTENTS

Key Cybersecurity Challenges for Healthcare

Lack of In-House Expertise

Many organizations struggle with a shortage of skilled cybersecurity professionals, which hampers their ability to effectively manage and respond to threats. This skill gap can lead to inadequate threat analysis and delayed incident response, increasing the impact of attacks. In fact, 90% of organizations reported a lack of skilled cybersecurity personnel, a gap expected to widen as threats become more complex.

Increasing Sophistication of Cyber Threats

Cyber threats are becoming more advanced, with attackers employing complex techniques such as zero-day and chained exploits. This sophistication makes detection and mitigation challenging for unprepared organizations. According to OCR, there has been a 93% rise in large data breaches from 2018 to 2023, along with a staggering 239% increase in hacking incidents during the same timeframe and a 278% surge in ransomware attacks targeting healthcare.

Limited Resources for Threat Monitoring

Security teams are overwhelmed by the sheer volume of alerts generated by various security systems. This constant influx of alerts can lead to desensitization, causing critical alerts to be overlooked or ignored. The high rate of false positives further exacerbates this issue, resulting in alert fatigue, team burnout and higher rates of human error leading to security incidents.

Response Time Delays

Slow incident response, often due to manual processes and alert fatigue, can amplify the impact of successful cyber attacks, allowing threats to spread and cause more harm.

Program Implementation and Maturity

Achieving maturity in threat detection and incident response capabilities demands significant investment in time and expertise, as teams must constantly navigate evolving cyber threats and emerging technologies. The complexity is compounded by the need for continuous training and adaptation to maintain high standards of security, meaning less time focused on core business initiatives to innovate healthcare access. As a result, many organizations struggle to reach the necessary level of operational maturity to effectively counter advanced threats, making external MDR services an attractive alternative for achieving comprehensive and timely security enhancements.

Alarming Stats from the Past Decade

Sheer Onslaught of Bad Actors

4,000
New cyberattacks each day

560,000
New pieces of malware detected each day

Every 14 seconds
Four times each minute, a company falls victim to a ransomware attack, resulting in devastating losses

Intolerance for Failure to Secure Data

60%
Small businesses that close after a cyber attack due to financial burden

70%
Consumers who said they'd stop doing business with a company after a data breach, highlighting severe reputational damage

Healthcare Sector Vulnerability

$3.86M
Non-Healthcare Orgs
Average cost of a cybersecurity breach

$7M
Healthcare Orgs
Average cost of a cybersecurity breach, in addition to risking lives, interruptions in care, and erosion of trust

Evaluating Your Cybersecurity Needs

DOES YOUR BUSINESS NEED...

Turnkey threat detection, investigation, and response capabilities	**Yes**	**No**
Proactive identification of threat exposures and preemptive security responses	**Yes**	**No**
Eradication and recovery support services	**Yes**	**No**
The capability to remotely initiate active containment or disruption of threats	**Yes**	**No**
24/7 remotely delivered, human-driven, AI-supported security operations and support services	**Yes**	**No**
Incident reporting and the option for manual or automated threat mitigation	**Yes**	**No**
Exposure management capabilities	**Yes**	**No**
Self-service technology capabilities	**Yes**	**No**
Compatibility with threats to modern infrastructure	**Yes**	**No**
MDR services compatible with multiple cloud service platforms	**Yes**	**No**
Compliance with healthcare regulatory requirements	**Yes**	**No**
Joint Incident Response Plan	**Yes**	**No**

If your answer is **YES** to any of the above, refer to **What to Ask a Potential Vendor Partner**

Go to **Section** ▶

Benefits of MDR for Healthcare Organizations

The best MDR solutions offer enhanced threat detection, compliance support, increased visibility, access to expertise, cost-effectiveness, and importantly, the flexibility to meet the unique needs of their customers. These benefits are pivotal for maintaining strong security postures.

Why is Healthcare Data So Vulnerable?

High-Value Data

Medical records hold crucial information, including personal identification, medical history, and financial details, making them highly sought after on the black market due to their multiplicity of use cases.

Regulatory Requirements

The need for healthcare organizations to meet compliance standards against regulations like HIPAA and HITRUST adds another layer of complexity that can be hard to achieve without specialized expertise and knowledge.

Complex Infrastructure

The integration of multiple systems and devices in healthcare settings increases the attack surface, creating more entry points to exploit.

How can a security breach happen?

In a typical scenario, Company A possesses a wealth of sensitive data and boasts a robust security program, ensuring that its applications and data are tightly secured. Company B, a business partner of Company A, has access to this protected dataset through a user account linked to Company A's database. However, if that account is compromised due to phishing, the attacker gains unauthorized access to the secure database solely because of the trusted relationship between the two organizations.

MDR guards against this scenario. Find out how ▶

Benefits of MDR for Healthcare

Detect, Prevent and Mitigate Cloud Threats

MDR solutions significantly bolster a healthcare organization's ability to safeguard sensitive patient data by swiftly identifying and responding to emerging threats. With advanced technologies such as machine learning and artificial intelligence, MDR providers deliver enhanced threat detection capabilities beyond traditional measures. This technological edge, combined with expert analysis, enables accelerated response times to neutralize threats before they can inflict damage. This helps maintain the integrity and confidentiality of healthcare data, and prevents incidents from diverting critical resources away from innovation.

Managed Compliance and Risk Reduction

MDR services play a crucial role in helping healthcare organizations thwart cyber-attacks, however, most are not built to address compliance with stringent regulations like HIPAA and HITRUST. The best solutions for healthcare ensure that all security practices align with legal requirements, effectively reducing the risk of non-compliance penalties by prioritizing vulnerabilities based on potential business impact and mitigating the risk as quickly as possible. When it comes to response and recovery, most MDR providers are adept at digital forensics and incident recovery to analyze what happened. However, almost all rely on the customer to remediate the issue. This gap leaves the customer at risk until they fix the issue. MDR partners capable of remediating on the customers' behalf increase the effectiveness of customers' security posture and reduce risk in near-real time.

Get More Visibility and Monitor Threats Proactively

MDR solutions offer a comprehensive view of an organization's entire IT infrastructure, facilitating proactive monitoring for potential threats. This holistic insight into endpoint, network, and cloud activity allows for early detection of anomalies and vulnerabilities, enabling healthcare organizations to preemptively address security risks. With enhanced network visibility, organizations can detect suspicious activities early, allowing timely interventions and reducing the likelihood of successful cyber attacks.

Expertise & Advanced Technologies

By partnering with an MDR provider, healthcare organizations gain access to specialized cybersecurity expertise and state-of-the-art technologies that may not be feasible to maintain in-house. MDR providers bring a wealth of experience and specialized skills that enhance threat detection and response capabilities, ensuring organizations are equipped to handle the complex and evolving landscape of cyber threats. Leveraging this external expertise allows healthcare providers to focus on core operations while ensuring robust security measures are in place.

Cost-Effectiveness

Outsourcing cybersecurity management to an MDR provider can significantly reduce costs compared to maintaining an internal security team. MDR services offer cutting-edge technologies and expert resources without the overhead expenses associated with hiring and training in-house cybersecurity staff. This cost-effective approach allows healthcare organizations to allocate resources more strategically while benefiting from high-quality security solutions.

Essential Attributes of an MDR Vendor Partner

Taking a closer look at the features, services, technologies, and holistic approach to protection behind an MDR solution are critical factors when evaluating potential vendor partners and software. Essential features of an MDR solution should include:

Defensive and Offensive Threat Detection & Response

Look for advanced technologies and features built in, like machine learning and behavioral analysis, that can hunt down and stop threats before they occur. Rapid response mechanisms need to be in place to proactively ensure that potential incidents are addressed before they escalate to breaches. If the MDR solution you're reviewing only mitigates and remediates threats once they've begun to impact your cloud ecosystem, seek out more proactive options.

In evaluating the effectiveness of an MDR solution, key performance indicators such as Mean Time To Investigate (MTTI) and Mean Time To Recovery (MTTR) play a crucial role. MTTI is the time it takes to detect, triage, and completely investigate (analyze) the threat, and MTTR assesses the time taken to recover from that threat. Lower values in both metrics indicate a more efficient and effective MDR solution, highlighting its ability to not only detect but also quickly act against potential security incidents.

Automated Incident Response & Remediation

Automation plays a pivotal role in streamlining incident response processes, allowing threats to be mitigated swiftly without heavy reliance on manual interventions. By automating routine tasks, MDR solutions reduce response times and minimize the risk of human error, thereby enhancing the overall efficiency and effectiveness of security operations. This not only allows security teams to focus on more strategic tasks but also ensures consistent and reliable threat remediation, which is crucial for maintaining a strong security posture in dynamic threat environments. On the other side of the coin, there are managed detection and response services that offer managed remediation and recovery for organizations that do not have robust security teams to remediate potential threats.

Extended Detection and Response (XDR) enhances automated incident response by providing a unified view of threats across various security layers, such as endpoints, networks, and servers. By integrating various security tools and automating responses, XDR minimizes manual intervention, reduces response times, and lowers the risks of human error.

24/7 Monitoring by Expert Security Analysts

Continuous monitoring by expert security analysts ensures that threats are detected and managed promptly, providing crucial insights and interventions as needed. With round-the-clock surveillance, organizations benefit from the expertise of professionals who are equipped to handle emerging threats with precision and speed. This constant vigilance offers peace of mind, knowing that security threats are actively managed, and strengthens the organization's defense against cyberattacks.

Integration with Existing Security Tools

An MDR solution that integrates seamlessly with existing security infrastructure maximizes strategic security posture efforts. Such integration allows for improved data flow and communication between security tools, enhancing overall security posture without the need for costly overhauls. This compatibility not only reduces operational complexity, but also leverages existing investments in security technologies, providing a more cost-effective and comprehensive solution for organizations striving to protect their data assets.

It's crucial for healthcare organizations to consider how their solutions integrate with existing security tools like Security Information and Event Management (SIEM), and Extended Detection and Response (XDR) systems. These integrations can significantly enhance data flow and communication, which are vital for a robust security posture.

Compliance with Industry Regulations (e.g., HITRUST)

In the healthcare sector, compliance with industry regulations like HIPAA and HITRUST are non-negotiable. An MDR solution that is specifically tuned to HITRUST is invaluable in prioritizing compliance-related issues, allowing organizations to focus resources on the most critical vulnerabilities, minimizing the burden on IT teams. By proactively identifying and addressing potential non-compliance threats, a HIPAA-tuned MDR mitigates risks of non-compliance, which enhances decision-making processes by providing clear insights into compliance gaps, enabling swift remediation actions.

Ultimately, this specialization not only fortifies the organization's security posture but also safeguards its reputation and trust within the healthcare community. Vendors should be able to demonstrate their adherence to relevant standards.

Cost Efficiency

Is an MDR solution cost effective for your organization? As the need for all-encompassing IT solutions grows, many MSSPs are broadening their scope to include MDR services. The merging of MDR and MSSPs offers multiple advantages for businesses and organizations.

First, the convergence of MDR and MSSP services in one partner simplifies the process of piecemealing your security and compliance solutions, minimizing the complexity of dealing with several vendors, and ultimately saving both time and money. Additionally, this approach promotes a more cohesive and efficient management of IT and security. Lastly, by collaborating with a single provider, businesses can guarantee that their IT and security solutions are seamlessly integrated, enhancing overall protection and patient safety.

What to Ask a Potential MDR Vendor Partner

QUESTIONS to ASK

Defensive and Offensive Threat Detection & Response

- How does your system detect threats in real time?
- What is the average response time to incidents?
- Can you provide case studies demonstrating how real-time detection made a difference in past incidents?

Automated Incident Response & Remediation

- What aspects of incident response are automated?
- How does your automation improve response times?
- Can your automation system be customized to fit our specific workflow?
- How do XDR and your integrated platforms enhance automated incident response and remediation in your security solutions?

24/7 Monitoring by Expert Security Analysts

- How many security analysts will be monitoring our systems?
- What qualifications and experience do your analysts have?
- How do you handle alerts received outside of regular business hours?

Integration with Existing Security Tools

- How does your MDR solution integrate with our current NDR, SIEM, and XDR tools?
- What steps do you take to ensure seamless compatibility without disrupting our existing security infrastructure?

Compliance with Industry Regulations (e.g., HITRUST)

- How does your solution ensure compliance with [specific regulation relevant to your healthcare organization]?
- Can you provide documentation of compliance?
- How do you stay up with changes in industry regulations?
- What processes do you have for incident response and reporting, including potential breaches of compliance?

Cost Efficiency

- Can you provide cost comparisons with in-house solutions?
- How about scalability and cost adjustments as our needs evolve?

Internal Evaluation

To aid in selecting the right MDR solution, consider rating the key features of your current solution with a table such as this. Prioritizing these features ensures comprehensive protection against cyber threats, offering organizations peace of mind in safeguarding sensitive data.

Feature	Strong	Okay	Weak
Real-time threat detection			
24/7 monitoring			
Automated & managed incident response & recovery			
Compliance with industry regulations			
Cost efficency			

A Step-by-Step Guide to Evaluating MDR Vendors

A clear evaluation process is key in selecting the right MDR vendor for your cloud compliance and cybersecurity. It's how you can effectively evaluate vendors, focusing on their threat detection technology, response times, support services, and compatibility with your specific requirements. Follow our guide to evaluate vendors against top criteria and assess their performance over time.

STEP 1

Conduct an Internal Audit

Begin by thoroughly assessing your current security posture. Review past incidents, evaluate the effectiveness of your existing security tools, and gather insights from your IT and security teams. This audit will help you identify areas where your defenses are strong and where improvements are necessary.

STEP 2

Identify any Security Gaps

Determine specific weaknesses that an MDR service can address. Focus on the types of threats you are most susceptible to and the security functions that need enhancement. Ensure that the MDR provider's offerings, such as advanced threat detection and continuous monitoring, align with these needs.

STEP 3

Engage Stakeholders for Alignment

Collaborate with key stakeholders, including executives and department heads, to ensure that the MDR solution aligns with your organizational goals. Discuss how partnering with an MDR provider can support risk management, digital transformation, or business continuity efforts.

STEP 4

Evaluate Compliance and Regulatory Support

Investigate how the MDR provider helps meet industry compliance standards relevant to your organization, such as GDPR or HITRUST. Review their data protection policies, audit capabilities, and reporting features to ensure they can help maintain compliance and adapt to regulatory changes.

STEP 5

Set Performance Metrics

Establish clear KPIs that reflect both your strategic goals and security needs. Regularly evaluate how well the MDR solution meets these objectives compared to other vendors. This ongoing assessment ensures you maximize your investment and make necessary adjustments.

STEP 6

Check for Scalability and Support

As your organization grows, ensure the MDR vendor can scale their solutions accordingly. Evaluate their customer support services, including response times and the availability of a dedicated support team. Reliable support is crucial for a strong vendor partnership.

STEP 7

Analyze Technology Integrations

Confirm the MDR provider offers tools for real-time compliance monitoring and aligns with your organizational objectives. Effective integration of these tools can help you quickly identify and address potential issues, ensuring seamless security operations.

Outline for Implementing an MDR Solution in a Healthcare Cybersecurity Company

1 Implementation

An effective MDR implementation requires engagement with key stakeholders to ensure regulatory compliance with healthcare regulations like HIPAA, HITECH, and GDPR, while also defining the budget and allocating resources, including personnel and technology, to develop a timeline with key milestones.

2 Integration & Training

When deploying an MDR solution, it's essential to choose the right provider by assessing their features, support, and healthcare expertise. Plan for seamless integration with existing IT and security systems, ensuring secure data transfer protocols are established and tested in a controlled environment before full deployment.

Additionally, conduct training sessions for IT staff and end-users on new processes and tools, develop a change management strategy to minimize disruption, and set up a support system to address user concerns and technical issues, ensuring a smooth transition and effective use of the MDR solution.

3 Monitoring & Optimization

Implement continuous monitoring for prompt threat detection, utilize threat intelligence, regularly evaluate performance against KPIs, conduct audits for compliance, gather stakeholder feedback, adjust processes based on evaluations, plan for scalability with growing data and evolving threats, and foster a culture of security awareness and continuous improvement within your organization.

Why ClearDATA MDR?

Compliance-Forward Security Innovation

At ClearDATA, we're all about empowering healthcare organizations to tackle compliance head-on and take control of their data. Our integrations with top-notch compliance frameworks like HIPAA, HITRUST, NIST, and ISO27001 don't just tick boxes—they actively safeguard your data, enhance integrity, and ramp up your audit preparedness. ClearDATA's MDR offering provides comprehensive and flexible monitoring, consistent audits, and ongoing support, has your healthcare cybersecurity needs covered. With ClearDATA, you'll notice a smoother, more efficient implementation of your policies in alignment with the strictest healthcare standards.

> "ClearDATA got us to market in the cloud months faster than we could have alone, and because we don't have a robust internal IT department, ClearDATA protects us."
>
> delegate

What do you get with ClearDATA MDR?

- ✓ A clear line of sight into your biggest threats and how to stop them.
- ✓ Shared intel that stops threats before they can strike your cloud.
- ✓ Threats neutralized 5x faster than if you did it alone.
- ✓ Your time back to focus while we handle your cloud cybersecurity protection

Choose Your Level of Protection Suited to Your Business Needs

At ClearDATA, we meet you where you are in your cloud journey.

MDR Basic

Encompasses the fundamental aspects of threat detection, ensuring that systems are continuously monitored for any irregular activities.

MDR Essentials

Offers an elevated level of surveillance, combining advanced analytics with incident response capabilities to swiftly address threats.

MDR Complete

The ultimate package. Provides comprehensive protection with continuous threat hunting, in-depth analysis, and guided remediation.

Holistic Approach To Healthcare Threat Mitigation

ClearDATA integrates both proactive and reactive strategies, leveraging cutting-edge monitoring tools to ensure robust threat coverage and rapid detection of potential breaches. Our team of dedicated experts constantly monitors for risks, empowering you to maintain your focus on delivering exceptional healthcare. With our comprehensive protection, you can operate with peace of mind, knowing your security challenges are expertly managed. Our team of dedicated experts is always on the lookout for risks, making sure you can focus on what you do best—delivering top-notch healthcare without worrying about security issues.

Prioritized Insights & Rapid Responses

ClearDATA MDR for healthcare elevates threat response by offering collaborative, proactive measures on behalf of healthcare organizations. Leveraging our advanced CyberHealth™ Platform, we transform chaos into clarity, providing not only the tools but also the expert guidance needed to swiftly and confidently tackle cybersecurity challenges while avoiding the debilitating effects of "alert fatigue." The platform integrates seamlessly with your cloud environments to offer real-time monitoring, detailed analytics, and customized alerts tailored to your specific needs.

Our defense mechanisms and unparalleled cybersecurity expertise ensure that your threat response and recovery times are up to five times faster than if managed independently. Additionally, we offer continuous support and training to keep your team updated on the latest security practices, ensuring a resilient and secure environment for your critical healthcare operations.

Shared Intelligence & Collaborative Action

At ClearDATA, we harness the power of collective intelligence from our vast network to keep healthcare data safe. Our Managed Detection and Response (MDR) service is designed to spot even the most elusive anomalies that might slip through the cracks otherwise. With a team of seasoned cybersecurity experts at the helm, we don't just stop threats in their tracks; we share our insights with the broader healthcare community. This collaborative 'network effect' boosts the security of patient information, benefiting not only our clients but the entire industry.

Our mission? *To provide ironclad protection tailored to your business needs in a complex, competitive healthcare industry.*

What sets ClearDATA MDR apart?

Healthcare Focus

ClearDATA focuses 100% of its time and effort on one sector — Healthcare

White Glove Onboarding

We make client onboarding seamless, integrating with your existing systems so you're secure and compliant on day one

Rapid Responses

On average, MDR clients can expect 5x quicker responses to security threats than in-house staff

Continuous Improvement

We gather, combine, and apply anonymized intelligence from every client under the ClearDATA dome

Experience the **ClearDATA Difference**

Enabled by the first and only software of its kind for healthcare, companies of all sizes gain full visibility, protection, and enforcement of security and compliance measures to secure PHI and other sensitive healthcare data in the cloud.

95 **CSAT** Score

"Excellent!" ★★★★★

THE RIGHT EXPERTISE

ClearDATA's software and services were designed from the ground-up with healthcare providers and partners in mind. Rest easy knowing the healthcare industry's rigorous compliance needs are covered.

HITRUST CSF Certified

HIPAA COMPLIANT

GDPR COMPLIANT

GxP Pharma Solutions

ITIL®

AICPA SOC

HIMSS North America PLATINUM Corporate Member

NIST

CIS SecureSuite® Membership

THE RIGHT SOLUTIONS

Whether you choose software-only or one of our managed services packages, ClearDATA's solutions can be tailored to your team's needs and work with the three major public cloud providers (AWS, Azure, and GCP) — which is exactly why healthcare organizations love them.

aws

THE CLEAR CHOICE

Continuous compliance. PHI protection. Healthcare-focused CSPM. Wherever you are on your healthcare cloud journey, **ClearDATA is the clear choice for success.**

Humana.

JOHNS HOPKINS MEDICINE

delegate

cleerly

Roche

everly health

MACHINIFY

CHORDLINE™ HEALTH

St. Jude Children's® Research Hospital

...and so many more

Reach out today to schedule a consultation with one of our experts, who will help you find the best solution for your organization's healthcare cloud compliance and security needs.

ClearDATA.com ☎ (833) 99-CLEAR

Schedule a Consultation

CLEARDATA®

©2024 ClearDATA. MKT-0173 Rev. A October 2024

CLEARDATA®

APPENDIX

The Alphabet Soup of Cybersecurity

Included as part of **Healthcare's Ultimage Guide to MDR** from ClearDATA. Feel free to print this out and keep it handy.

Cybersecurity Acronyms

The healthcare sector alone is filled with many acronyms that are significant in the realm of patient privacy, protection, and portability. Let's explore the basic acronyms your healthcare organization should be aware of. Understanding the different attributes and features is effectiveness.

SIEM (Security Information and Event Management) — SIEM systems consolidate and analyze security data across an organization's IT infrastructure. They are crucial for real-time threat identification and response, offering insights through the aggregation of logs and security events to detect anomalies and potential threats.

SOC (Security Operations Center) — A SOC is a dedicated, centralized unit tasked with handling an organization's security issues at both technical and organizational levels. It plays a vital role in monitoring, detecting, and responding to cybersecurity incidents, ensuring a proactive security posture.

EDR (Endpoint Detection and Response) — EDR solutions focus on threats targeting endpoint devices, providing detailed visibility and analysis of endpoint activities. They are essential for detecting, investigating, and responding to threats, enhancing the ability to protect against advanced attacks.

MTTI (Mean Time To Investigate) — the speed at which a threat detection notice is transformed into a comprehensive investigation (the team has assessed the alert and carried out the investigation before handing over responsibility to the client for remediation).

MTTR (Mean Time To Respond) — the duration it takes for the client to fully remediate or resolve an escalated incident after being notified.

NDR (Network Detection and Response) — NDR emphasizes monitoring network traffic to detect and respond to threats. It is crucial for identifying suspicious activities and preventing network-based attacks, providing an additional layer of defense by analyzing traffic patterns and anomalies.

Healthcare-Specific Acronyms

PHI (Protected Health Information) — Any information in a medical record or other healthcare setting that can be used to identify an individual and is created, used, or disclosed while providing healthcare services.

HIPAA (Health Insurance Portability and Accountability Act) — A U.S. law that establishes standards for protecting sensitive patient data and ensures the privacy and security of PHI.

HITECH (Health Information Technology for Economic and Clinical Health Act) — Legislation that promotes the adoption and meaningful use of health information technology, enhancing HIPAA's privacy and security protections.

HITRUST (Health Information Trust Alliance) — A cybersecurity framework developed specifically for healthcare organizations to comply with various regulations such as HIPAA and HITECH.

EHR (Electronic Health Record) — A digital version of a patient's medical history maintained by healthcare providers, including PHI.

EMR (Electronic Medical Record) — Similar to EHR but typically refers to the internal record of health-related information kept within a single healthcare provider's system.

BAA (Business Associate Agreement) — A contract required under HIPAA that outlines responsibilities and safeguards between a healthcare provider and a third-party service handling PHI.

NIST (National Institute of Standards and Technology) — A federal agency that provides cybersecurity frameworks and standards, which are frequently used by healthcare organizations to secure their systems.

OCR (Office for Civil Rights) — A division of the U.S. Department of Health and Human Services that enforces HIPAA compliance and investigates data breaches in healthcare.

HIE (Health Information Exchange) — A system that allows healthcare providers to electronically share a patient's medical information across different organizations securely.

Continued ▶

Glossary *of* Acronyms

CLEARDATA®

BAA	Business Associate Agreement
BAS	Breach Attack Simulation
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CPS	Cyber-Physical Systems
CTEM	Continuous Threat Exposure Management
DFIR	Digital Forensics and Incident Response
DLP	Data Loss Prevention
EDR	Endpoint Detection and Response
EHR	Electronic Health Record
EMR	Electronic Medical Record
GDPR	General Data Protection Regulation (for EU healthcare data protection)
HHS	Department of Health and Human Services
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
HITRUST	Health Information Trust Alliance
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IDS	Intrusion Detection System
IoT	Internet of Things (relevant in medical devices)
IPS	Intrusion Prevention System
IRP	Incident Response Plan
MDR	Managed Detection and Response
MFA	Multi-Factor Authentication
MSSP	Managed Security Services Provider
MTTI	Mean Time to Investigate
MTTR	Mean Time to Respond
NDR	Network Detection & Response
NIST	National Institute of Standards and Technology
OCR	Office for Civil Rights
OT	Operational Technology
PCI DSS	Payment Card Industry Data Security Standard
PHI	Protected Health Information
POC	Proof of Concept
RFP	Request for Proposal
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SI	Systems Integrator
SIEM	Security Information and Event Management
SOC	Security Operations Center
SOC 2	Service Organization Control 2
TDIR	Threat Detection, Investigation, and Response
TI	Threat Intelligence
TTPs	Tactics, Techniques, and Procedures