FIELD EFFECT

Covalence Compliance Series

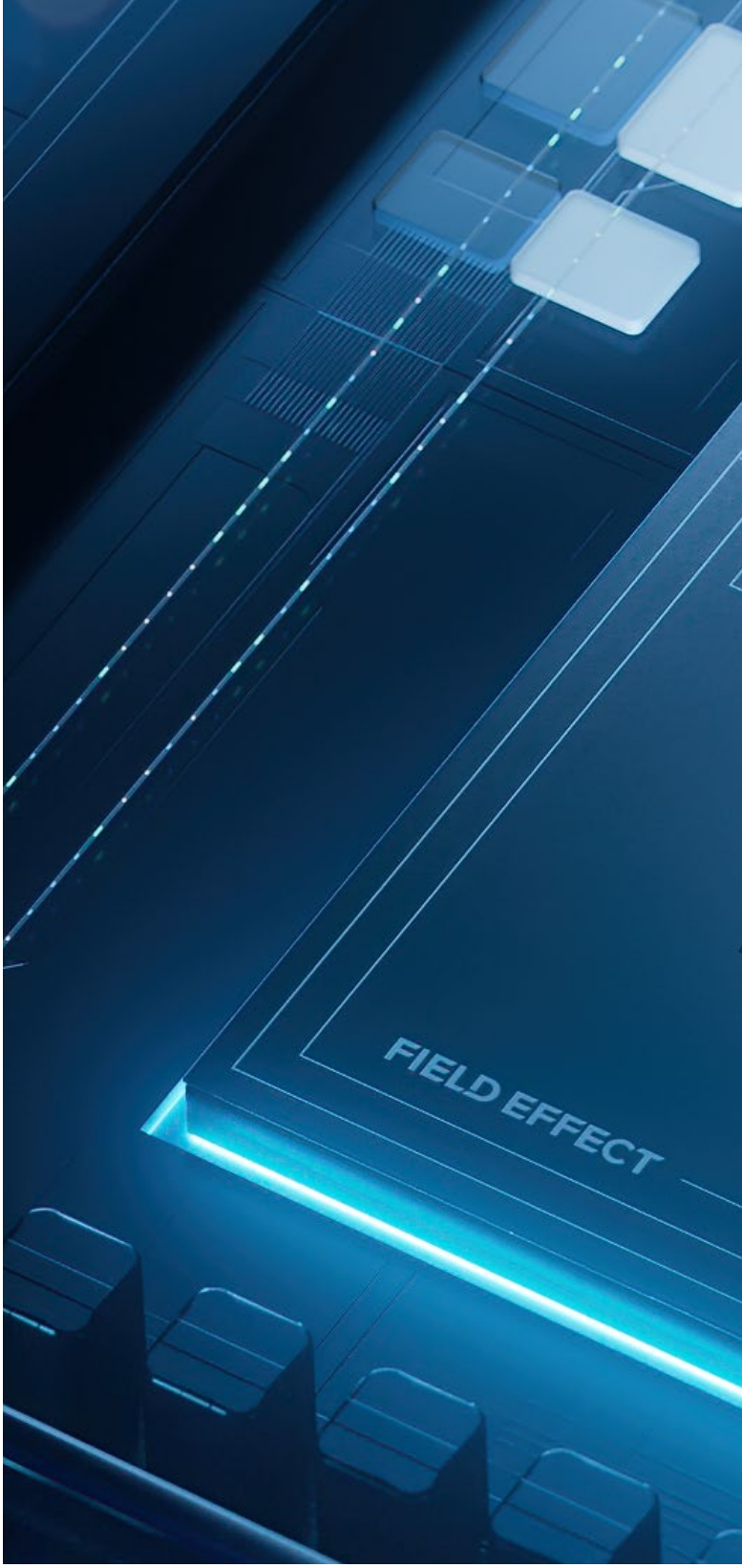
MAPPING GUIDE

HIPAA

About Field Effect

Field Effect, a global cybersecurity company, is revolutionizing the industry by bringing advanced cybersecurity solutions and services to businesses of all sizes. After years of research and development by the brightest in the business, we have pioneered a holistic approach to cybersecurity.

Our complete Managed Detection and Response (MDR) solution, flexible simulation-based training platform, and expert-led professional services form a unified defense that results in superior security, less complexity, and immediate value. We build solutions that are sophisticated, yet easy to use and manage, so every business owner can get the hands-free cybersecurity they expect. For more information, visit fieldeffect.com.



About HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996. Its goal was to modernize the flow of healthcare information, protect personally identifiable information maintained by the healthcare organizations from fraud and theft, and address some limitations on healthcare insurance coverage. Field Effect is happy to support our healthcare clients with this guide, which shows how our flagship product (Covalence) can satisfy certain HIPAA requirements and help streamline the implementation process.

* This document is intended to help readers better understand the regulatory compliance landscape and its potential obligations, and does not replace or negate official guidance from an auditor. Consulting a regulatory auditor or similar authority is recommended for specific guidance on your organization's compliance requirements.

HIPAA Section	HIPAA Clause	HIPAA Full Text	Covalence Description
164.306	**A1**	Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	By identifying known threats and anomalous events, Covalence provides holistic security to help protect the confidentiality, integrity, and availability of electronic protected health information (EPHI).
164.306	**A2**	Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.	Covalence employs industry standard IOCs along with our own threat intelligence to identify malicious systems, domains, botnets, ransomware, and other threats to your environment.
164.308	**A3**	Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Covalence monitors for the unauthorized disclosure and extraction of information (e.g. SharePoint sites, removable media) and has the ability to lock cloud accounts and endpoint devices to prevent data leakage. Covalence monitors login activity and detects system access from anomalous locations.
164.308	**A4**	Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	See above.
164.308	**A5**	Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.	Covalence provides world-class, holistic protection against malware on the endpoint, network, and cloud. In addition to identifying key indicators of system breaches prior to malware execution, Covalence can block malicious software and isolate devices until the full extent of the risk is assessed.

HIPAA Section	HIPAA Clause	HIPAA Full Text	Covalence Description
164.308	**A5**	Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	Covalence monitors for suspicious login attempts, and can be configured as a log receiver to monitor login events from devices that are unable to install the endpoint agent.
164.308	**A6**	Standard: Security incident procedures. Implement policies and procedures to address security incidents.	Covalence provides real-time detection and in-depth situational awareness that allows organizations to refine their security policies and procedures. In addition, Field Effect offers vCISO services, including a detailed Incident Response Preparedness package, with optional Table Top exercises to test the policies and procedures in a mock security incident situation.
164.308	**A6**	Implementation specification: Response and reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	Covalence identifies and takes appropriate action to prevent information security incidents, and is powered by sophisticated, scalable technology, and a dedicated team of cybersecurity analysts. Covalence AROs help organizations track and document security incidents without the deluge of threat alerts common to nearly all other cybersecurity products. The Covalence Suspicious Email Analysis Service (SEAS) is an Outlook add-on that provides users the ability to request automated analysis of suspicious email to help them report security incidents.
164.312	**A1**	Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Covalence detects anomalous login activity to help ensure that only authorized users access EPHI. Covalence can maintain an allow/block list of USB media, which helps ensure these devices are only leveraged when there's an organizational reason for their use.

HIPAA Section	HIPAA Clause	HIPAA Full Text	Covalence Description
164.312	B	Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Covalence collects logs of system activity and compares them against available threat intelligence, known behavior patterns, and malware signatures.
164.312	C	Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Covalence helps protect EPHI from improper alteration and destruction by monitoring for malware and unauthorized system access.
164.312	E1	Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Covalence monitors for system and network vulnerabilities that can put EPHI at risk, such as the use of legacy or insecure transmission protocols.

The most sophisticated cyber threat monitoring on the planet, made simple.

Covalence is an award-winning cybersecurity solution that provides transparent, holistic managed detection and response for your whole IT infrastructure in one platform, no matter where you are or where your endpoints are located. No add-ons, no modules, and no gaps in your security. Learn more about Covalence.

Covalence

About Field Effect

Field Effect believes that businesses of all sizes deserve powerful cybersecurity solutions to protect them.

Our threat monitoring, detection, and response platform, along with our training and compliance products and services are the result of years of research and development by the brightest talents in the cybersecurity industry. Our solutions are purpose-built for SMBs and deliver sophisticated, easy-to-use and manage technology with actionable insights to keep you safe from cyber threats.

Contact our team today.

Email:
letschat@fieldeffect.com

Phone:

CANADA + UNITED STATES
+1 (800) 299-8986

UNITED KINGDOM
+44 (0) 800 086 9176

AUSTRALIA
+61 1800 431418