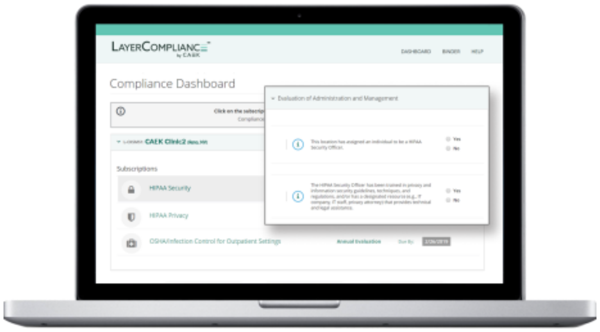
CASE STUDY

LAYERCOMPLIANCE™ by CAEK


LAYERCOMPLIANCE by CAEK

Compliance Dashboard

CAEK Clinic2

Subscriptions

Evaluation of Administration and Management

This location has assigned an individual to be a HIPAA Security Officer. ○ Yes ○ No

The HIPAA Security Officer has been trained in privacy and information security guidelines, techniques, and regulations, and/or has a designated resource (e.g., IT company, IT staff, privacy attorney) that provides technical and legal assistance. ○ Yes ○ No

LAYERCOMPLIANCE™ by CAEK

Ransomware Breach and OCR Investigation

THE STORY:

An office-based, healthcare practitioner suffered a ransomware attack that encrypted patient information on the practice's servers. Based on the Health and Human Services' guidance[1] on Ransomware, the practitioner investigated the security incident and determined it to be a breach. The practitioner followed the Breach Notification Rule and notified patients, the media, and the Secretary of Health and Human Services.

THE CHALLENGE:

Following the breach notification, the practitioner was notified by the Office for Civil Rights (OCR) that an investigation had been opened, and the practitioner received a detailed data request from OCR. The practitioner had 30 business days to respond to the data request, which included more than 20 separate items, along with documentation for specific standards and implementation specifications of the HIPAA Security Rule.

While most healthcare practitioners are prepared to provide documentation of policies and procedures and employee training, other requests for detailed documentation and evidence of the implementation of specific parts of the HIPAA Security Rule can prove challenging if there is no process to regularly document HIPAA activities.

RESPONSE USING LAYERCOMPLIANCE:

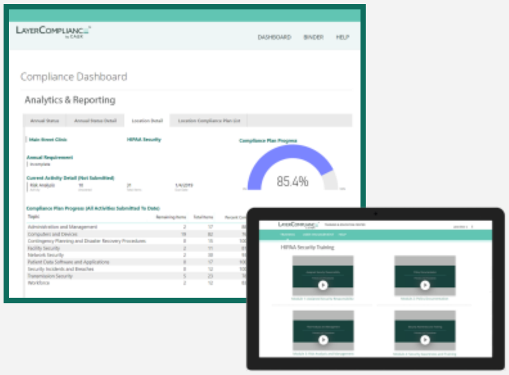
Using the LayerCompliance software, CAEK assisted the practitioner in implementing a HIPAA compliance process that included a risk analysis, revised policies and procedures, and an ongoing risk management plan to periodically review the implementation of the policies and procedures that address the HIPAA Privacy, Security, and Breach Notification regulations. The practitioner was able to provide a timely response to the OCR data request using the documentation from the LayerCompliance software for HIPAA activities performed after the incident and an extensive review by CAEK of documentation prior to the incident.

THE OUTCOME:

Based on the response provided to OCR using the documentation from LayerCompliance, the case was closed without further action and no fines were issued.

PARTIAL REQUEST FROM OCR

- Copy of the **policies and procedures** for safeguarding protected health information, in effect both at the time of the incident and currently.
- Evidence of staff training on policies and procedures prior to the security incident, and any training that occurred after the incident.
- Copy of the **risk analysis** in effect at the time of the incident and the current risk analysis.
- Copy of the **risk management plan** to reduce the risks identified in the risk analysis, including evidence of security measures implemented, in effect both at the time of the incident and currently.
- Documentation that the Covered Entity **implemented procedures** to regularly review records of information system activity, such as audit logs, access reports, and **security incident training reports**.
- **Evidence of the implementation** of hardware, software, and/or procedural mechanisms that record and examine activity in the Covered Entity's information systems that contain or use ePHI.


LAYERCOMPLIANCE by CAEK

Compliance Dashboard

Analytics & Reporting

Compliance Plan Progress (All Activities Submitted To Date)

Topic	Remaining Items	Total Items
Administration and Management	2	17
Computers and Devices	19	82
Contingency Planning and Disaster Recovery Procedures	0	15
Facility Security	2	11
Network Security	2	38
Patient Data Software and Applications	0	17
Security Incidents and Breaches	0	12
Transmission Security	5	23
Workforce	2	12

HIPAA Security Training

[1] https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

OCR INVESTIGATES PATIENT COMPLAINTS AND BREACHES OF ALL SIZES

Large breaches, affecting 500 individuals or more, are reported almost every day and posted on OCR's breach reporting site.[1]

Even breaches that affect less than 500 patients may be investigated by OCR and result in fine. For instance, in June 2016 a $650,000 settlement was reached for a lost mobile device that only affected 412 individuals[2].

Additionally, OCR receives tens of thousands of patient complaints each year. In 2017 alone, OCR received over 24,000 complaints.[3]

Depending on the breach, patient complaint, or other type of incident that triggers an OCR investigation, OCR may request documentation or evidence of implementation for any of the HIPAA Privacy, Security, and Breach Notification Rule regulations.

A COMPLIANCE PLATFORM FOR TODAY'S HEALTHCARE

Healthcare organizations may be required to respond to an OCR investigation at anytime due to a breach, patient complaint, or audit. Information will be requested for documentation in place prior to the incident or audit.

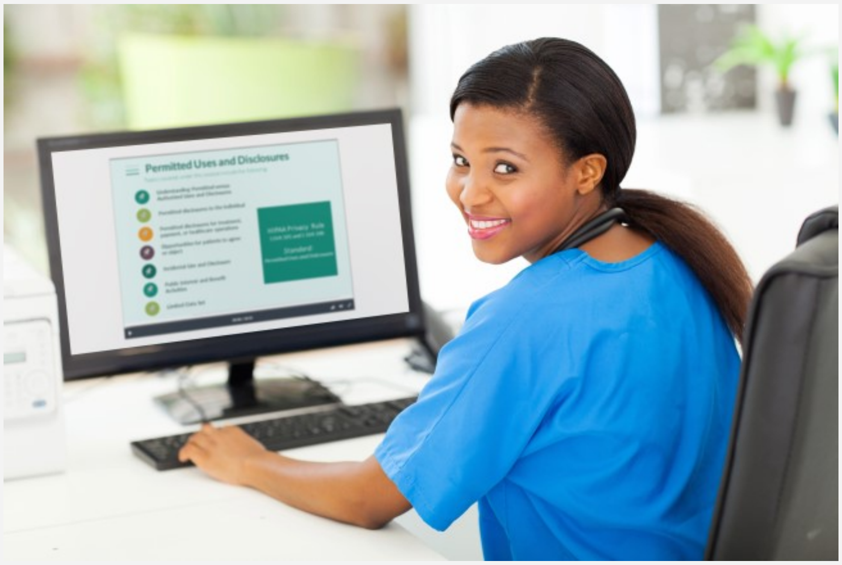
LayerCompliance platform automates compliance processes, tracks activities, and generates documentation, which leads to reduced risk.

- Tailored Digital Policies
- Online Training for HIPAA and OSHA
- Tracking and Oversight Dashboard
- Automates Compliance Processes
- Provides automatic task reminders
- Expert Support

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[2] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.

[3] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/complaints-received-by-calendar-year/index.html.



Contact an account manager to get started today.

800.334.6071
sales@layercompliance.com
www.LayerCompliance.com

ABOUT CAEK

CAEK®, Inc. is a Software-as-a-Service (SaaS) company providing compliance software for the healthcare industry through its flagship product, LayerCompliance®. LayerCompliance provides cost-effective compliance tools—including HIPAA and OSHA & Infection Control—for healthcare providers, other covered entities, and business associates.

www.LayerCompliance.com

LAYERCOMPLIANCE™
by CAEK