cognizant®

Healthcare vendor

Compliance Code of Conduct 2025

Contents

Vendor compliance

Cognizant is dedicated to complying with all applicable laws, regulations and company policies. Cognizant healthcare vendors play an integral part in achieving these goals and are expected to abide by a high standard of ethical behavior at all times, obeying all applicable rules and regulations.

Specifically, we are required to comply with the provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH) and Health Insurance Portability and Accountability Act (HIPAA). As such, privacy and security rules and all applicable state and local privacy and security laws are considered as part of our vendor oversight program and addressed in our vendor risk assessments.

Target audience and purpose

Cognizant's high-risk healthcare vendors (vendors) who handle, or have access to, our customer member protected health information (PHI), systems or sensitive information are required to abide by all relevant healthcare regulatory requirements and contractual obligations. This document describes the policies, training, background checks, documentation, security measures and formal attestation requirements for our vendors.

Compliance helpline

The Cognizant Ethics and Compliance Helpline is a convenient and anonymous way for vendors to report suspected wrongdoing, including fraud, waste and abuse (FWA), safety concerns and compliance violations, without fear of retaliation. It is available 24 hours a day, 365 days a year. Our toll-free compliance helpline number is 1-866-824-4897 or incidents can be reported to https://www.cognizant.com/compliance-helpline.

Cognizant will investigate any reports of those found to have violated applicable laws or Cognizant policies and procedures. The Cognizant Whistleblower and Non-Retaliation Policy, and federal law, protects "whistleblowers," those who report noncompliance or fraud, or assist in investigations, from retaliation.

What is a business associate?

A business associate (BA) is any entity who creates, receives, maintains or transmits PHI on behalf of a covered entity (CE) for a function or activity regulated under HIPAA. Functions and activities performed on behalf of clients involving the use or disclosure of individually identifiable health information, include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing.

What is a covered entity?

A covered entity means:

1. A health plan
2. A health care clearinghouse
3. A health care provider who transmits any health information in electronic form in connection with a transaction (i.e., claims, benefit inquiries, or payment processing) for which the Department of Health and Human Services (HHS) has established national HIPAA standards.

What is protected health information?

Protected health information is individually identifiable health information transmitted by electronic media; maintained in electronic media; and transmitted or maintained in any other form or medium, including demographic data related to:

1. An individual's past, present or future physical or mental health or condition
2. The provision of health care to the individual
3. The past present or future payment for the provision of health care to the individual
4. Information identifying the individual or for which there is a reasonable basis to believe it can be used to identify the individual or for which there is a reasonable basis to believe it can be used to identify the individual

Cognizant maintains, reviews and analyzes vendor risk and contracted responsibilities to determine vendor status, utilizing CMS evaluation criteria:

- Is the vendor providing administrative or healthcare services related to Medicaid, Medicare Part C or Part D plans?
- Does the vendor have access to or work with Cognizant customer's member data?
- Risks identified in annual questionnaire.

Oversight requirements

Accountability resides with Cognizant for any functions or responsibilities delegated to a vendor. As such, Cognizant is required to appropriately identify vendors and ensure the following:

- Maintain an accurate and current record of active and inactive associates who support the Cognizant account
- Complete federal, and any required state level, entity checks prior to hire and monthly thereafter
- Conduct appropriate general compliance and FWA training (at the time of contract, new employment and annually thereafter), and ensure that vendor annually attests in writing to completion of this required training

Vendor requirements

PHI/PII vendors and incidental access vendors—Compliance

- Have proper controls in place surrounding protected health information and attest to same (where applicable)
- Ensure employees, if such training is applicable, are provided with CMS and HIPAA compliance and FWA training upon hire, and annually afterwards, which vendor will attest to annually
- Have a documented records retention policy and document retention schedule and ensure compliance with same
- Conduct OIG/GSA background checks upon hire and monthly thereafter for all employees who support the Cognizant account
- Conduct background checks against the required state databases and any other exclusion lists specified in applicable state Medicaid contracts entered into by Cognizant clients
- Utilize and require its subcontractors to use the US Department of Homeland Security E-Verify system and procedures to determine the eligibility of all persons employed by the vendor or vendor's subcontractor(s) to perform any services for Cognizant
- Document process for resolution of issues or noncompliance, including description of specific penalties up to, and including, termination

- If your organization utilizes offshore facility or personnel for handling, storage, access and review of PHI, vendor will be required to complete the Cognizant Supplier Offshore/Subcontractor Attestation and provide a detailed description of the services and locations
- Vendors must provide proof of the above items upon request in a timely manner

Compliance program

Cognizant requires all vendors performing services as a business associate to Cognizant to attest, to the best of their knowledge and belief, that they have met the following compliance requirements:

1. Vendor has implemented written policies and procedures, and maintains a core values and standards of business conduct (code of conduct), which states the overall principles and values by which vendor operates; defines vendor's compliance expectations; provides that employees conduct themselves in an ethical manner; provides guidance on how to communicate compliance issues to compliance personnel and how those will be addressed; includes a policy of non-intimidation and non-retaliation; and provides guidance on handling conflicts of interest. Employees are required to acknowledge and agree to comply with the code of conduct upon hire and annually thereafter.
2. Vendor has a named compliance officer and compliance committee who report directly, and are accountable, to the chief executive officer, and who report to their governing body on the activities of the compliance program.
3. Vendor has established, implemented, and provides HIPAA privacy and security rules training, general compliance and fraud, waste and abuse training (if applicable) for employees, including temporary workers and volunteers, (collectively "workforce members"), upon hire and annually thereafter.
4. Vendor has established effective methods to communicate information from its compliance officer to its workforce members, which includes mechanisms to receive, record, respond to and track compliance questions or reports of suspected or detected noncompliance or potential FWA. These mechanisms are widely publicized and emphasize vendor's policy of non-intimidation and non-retaliation, and allow anonymous and confidential good faith reporting, on a 24- hour basis, of issues as they are identified.
5. Vendor has established and published disciplinary standards through the implementation of policies and procedures which encourage good faith participation in its compliance program.
6. Vendor has established a system for routine monitoring and identification of compliance risks in order to evaluate the effectiveness of its compliance program, including a risk assessment, monitoring and auditing, and remediation, of compliance and FWA risk areas.

7. Vendor screens its workforce members against the OIG and GSA exclusion lists upon hire by vendor and monthly thereafter. If any such workforce member is listed as an excluded individual on either list, vendor will take appropriate corrective action.
8. Vendor has established procedures and a system for promptly responding to compliance issues as they are raised, investigates potential compliance problems as identified, corrects such problems promptly and thoroughly to reduce the potential for recurrence, and ensures ongoing compliance.
9. Vendor has established a records information management policy which requires that compliance and training related materials be retained for a period of 10 years.

Vendor-required notifications

The following must be disclosed to the Cognizant compliance team immediately, upon hire, or if they are implemented later during the contract:

- Any exception to HIPAA requirements
- Utilization of an additional, subcontracted vendor to support Cognizant account
- Data storage in a cloud environment
- Any use of any offshore facility or personnel for handling, storage, access, review of PHI or as a recovery site
- Incident notification—in the event of a business interruption, or identification of any incident which impacts business operations, exposes PHI, or results in an SLA or quality impact to work product, vendor is required to notify Cognizant in accordance with its contractual requirements, ensuring Cognizant is notified promptly and provided with resolution and a description of the impact to Cognizant's customers' business

Frequency of vendor risk assessments and audits

Cognizant will conduct annual reviews of existing vendors to determine the type of assessment or validation of controls that will occur for that year.

Vendors will be provided with an annual compliance questionnaire and may be asked for additional information or documentation. Vendors will also be required to sign annual attestations of required HIPAA and FWA training, policies and procedures.

Identified issues will be provided back to the vendor in a corrective action (CAP) report. In some cases, an audit may be requested which may include members of the business team, security, compliance and legal teams. These audits may include site visits, if warranted.

Vendors will receive our annual questionnaire or attestation form by email, either as an Excel file or a link to MS Forms.

Annual compliance questionnaires

To ensure Cognizant has current compliance information for healthcare vendors, completion of an annual compliance questionnaire and supporting program documentation will be required each year. These questionnaires will request information related to many aspects of compliance, including:

- Operational practices
- Data handling and storage
- Compliance program
- Offshore operations
- Reporting mechanisms
- Healthcare regulatory compliance training
- Regulatory compliance-exclusion screening

Questions may include:

- Does vendor have all required compliance program documentation and practices in place?
- Is any part of the business subcontracted to a third party?
- Will any portion of our business, data storage, access, recovery plans or subcontractor be offshore?
- Does vendor conduct compliant mandatory annual HIPAA training?
- Does vendor conduct monthly OIG/GSA employee background checks?

Vendors are also required to sign the attestation, to ensure compliance with mandatory policies, procedures and training.

Communications

In the event of a business disruption, or to notify Cognizant of any incident impacting our business interests, please contact your Cognizant business contact and notify the compliance office at **chiefcomplianceofficer@cognizant.com**

Stay informed

Please contact the Cognizant Healthcare Business Unit Compliance Office with questions about this compliance program, policies, rules, regulations or training and documentation requirements. Send your inquiries to **edna.hernandez2@cognizant.com** or **arthur.myers@cognizant.com.**