



Healthcare vendor

Compliance Code of Conduct
2026

Contents

03

**Vendor
compliance**

04

**What is a
covered entity?**

05

**Vendor
requirements**

08

**Frequency
of vendor risk
assessments
and audits**

12-13

**Vendor Responsible
AI Requirements**

03

**Compliance
helpline**

04

**What is
protected health
information?**

06

**Compliance
program**

09

**Annual
compliance
questionnaires**

14

**Communications
Stay informed**

04

**What is a business
associate?**

05

**Oversight
requirements**

07

**Vendor-required
notifications**

10-11

Responsible AI

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 repricing.

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

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 PHI 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.
- Have policies in place that prohibit bribes, kickbacks, facilitation payments, improper gifts, entertainment, donations, sponsorships, referrals or other items of value intended to influence healthcare business, government officials, healthcare professionals, payers or procurement decisions.
- Screen workforce members who support the Cognizant account and, where required, contractors against the US Department of Health and Human Services Office of Inspector General List of Excluded Individuals and Entities (LEIE), the General Services Administration System for Award Management (SAM) and any other exclusion databases required by applicable law, regulation, contract or government healthcare program requirements. Screening shall occur prior to assignment and monthly thereafter or at intervals required by applicable law or contract.
- 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 designated personnel responsible for the oversight of its compliance program, with appropriate authority and organizational independence to carry out compliance responsibilities.
3. Vendor has established, implemented and provided 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 who support the Cognizant account, and where required, against the OIG and GSA exclusion lists prior to assignment 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 the period required under applicable law, regulation, contractual obligation or vendor policy, but in no event less than the minimum period required by applicable law.

Vendor-required notifications

Vendors supporting Cognizant Healthcare or Trizetto® Provider Solutions (TPS) must promptly notify the Cognizant Compliance Department of any event, change or condition that may affect the vendor's ability to meet contractual, regulatory, privacy, security, operational or service delivery obligations. Immediate reporting allows Cognizant to evaluate potential risk, determine whether additional review is required and take appropriate steps to protect clients, members, patients, data, systems and business operations.

The following must be disclosed 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
- Ownership and corporate structure
 - Change in ownership, merger, acquisition or divestiture
 - Change in company name or legal entity structure
 - Bankruptcy filing or insolvency proceedings
 - Significant changes in financial condition (credit downgrade, major losses)
- Security and data
 - Any data breach, security incident or unauthorized access involving our data
 - Material changes to your information security program or controls
 - Changes to encryption standards or data handling practices
 - Loss of relevant security certifications (SOC 2, ISO 27001, PCI-DSS, etc.)
- Subcontracting/Fourth-party risk
 - Use of new subcontractors or fourth-parties, especially if they'll touch our data or perform outsourced functions
 - Change in offshore/nearshore processing locations
 - Change in cloud service providers or key infrastructure vendors
 - Compliance and legal
 - Regulatory actions, fines, sanctions or investigations

- Litigation that could materially affect your ability to perform
- Loss or lapse of required licenses, permits or certifications
- Changes in regulatory status (e.g., becoming subject to new regulations)
- **Insurance**
 - Material changes to insurance coverage (cyber liability, E&O, general liability)
 - Lapse, cancellation or nonrenewal of required policies
- **Operational**
 - Key personnel changes (especially if a named individual/team was part of the deal)
 - Changes in business continuity/disaster recovery plans
 - Significant changes in service delivery locations
 - Material changes in financial viability (layoffs, location closures, etc.)
- **Product/Service**

Material changes to the product or service scope

- Changes in pricing structure tied to risk (if relevant)
- End-of-life or discontinuation notices for products/services you rely on
- Personnel and access
- Changes in background check or vetting standards for staff with access to our systems/data
- Changes in employee turnover that could affect service quality

The notification should include the date the issue was discovered, a summary of what happened, the impacted services, systems, data, clients or locations, any known or suspected regulatory impact, actions already taken and the vendor's planned next steps.

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 and changes
- Data handling and storage
- Compliance program
- Offshore operations
- Reporting mechanisms
- Healthcare regulatory compliance training
- Regulatory compliance exclusion screening
- Responsible AI principles/requirements

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.



Responsible AI

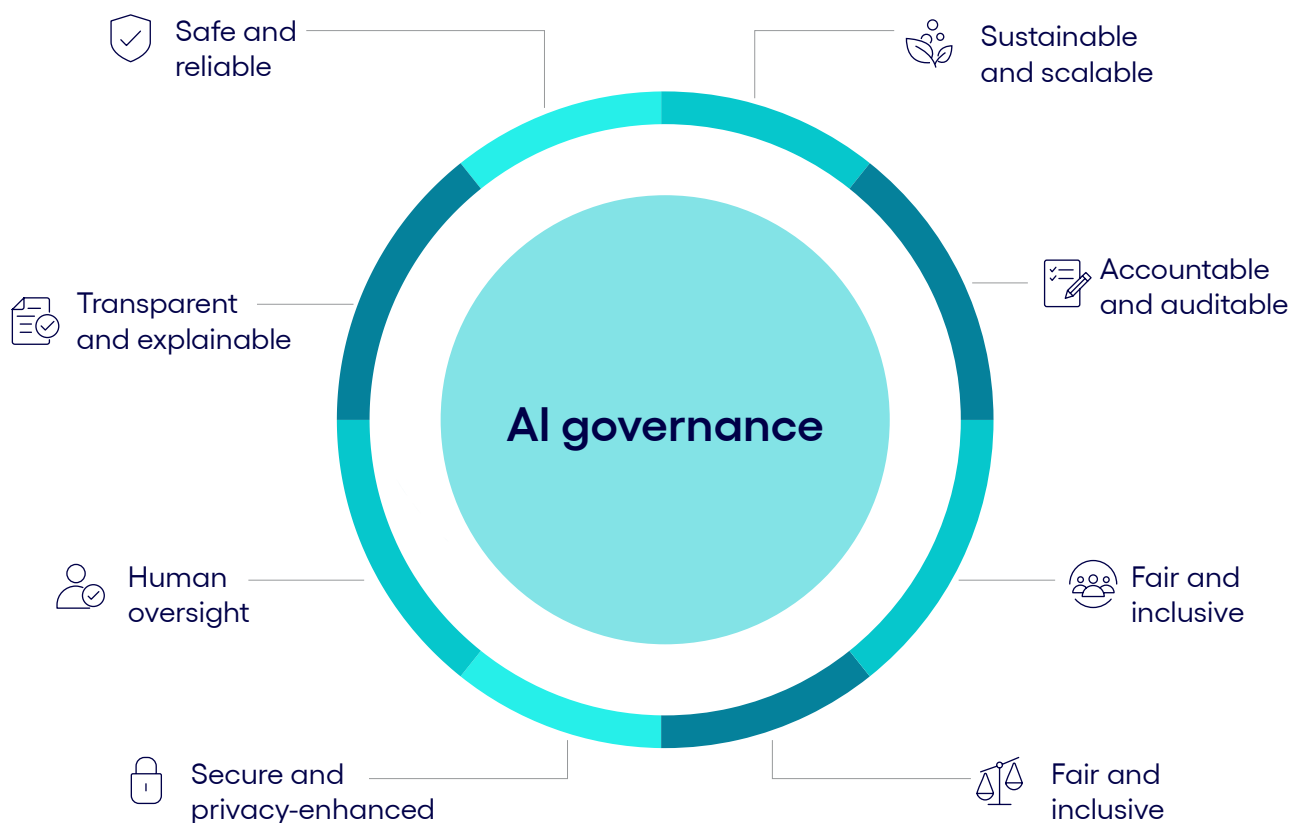
Cognizant is committed to advancing artificial intelligence (AI) in ways that are ethical, safe and trustworthy across the full AI lifecycle, guided by the Cognizant Responsible AI Policy and operationalized through Cognizant's Trust Framework.

Because vendors supporting Cognizant healthcare business frequently handle Cognizant data and Cognizant client data including protected health information (PHI), personally identifiable information (PII) and payment card information (PCI), the responsible use of AI is a core compliance expectation. Any vendor that develops, deploys, uses, procures or integrates AI or automated decision-making tools in connection with services provided to Cognizant is expected to uphold responsible AI standards equivalent to those set out in the Cognizant RespoWnsible AI Policy.

For purposes of this handbook, "artificial intelligence" means software, hardware or embodied agents that process information and learn through various computational techniques to generate output such as predictions, recommendations, decisions or actions based on human-defined or system-derived objectives.

Responsible AI principles

Cognizant's Responsible AI Policy is built on seven principles. Vendors are expected to apply these same principles, as applicable, to any AI used in delivering services to Cognizant:





Safe and reliable

AI systems are designed to perform as intended, with robustness testing and monitoring to prevent harm to people, property or the environment.



Transparent and explainable

The purpose, data use, limitations and reliability of AI are documented; AI-generated content is labeled where required; and meaningful explanations are available where AI may affect an individual's rights, health or safety.



Human-empowered

Human oversight and feedback are embedded across the AI lifecycle so that people remain in control of AI systems and outcomes.



Secure and privacy-enhanced

Personal information is protected throughout the AI lifecycle using privacy-enhancing technologies, data protection impact assessments, threat modeling, access controls, traceability and incident response.



Fairness and inclusivity

Bias is actively detected and mitigated, datasets are validated and systems are designed to be accessible and to produce equitable outcomes.



Accountable and auditable

Clear roles and responsibilities for AI oversight are assigned, misuse is prevented and systems are auditable for alignment with responsible AI principles and applicable regulations.



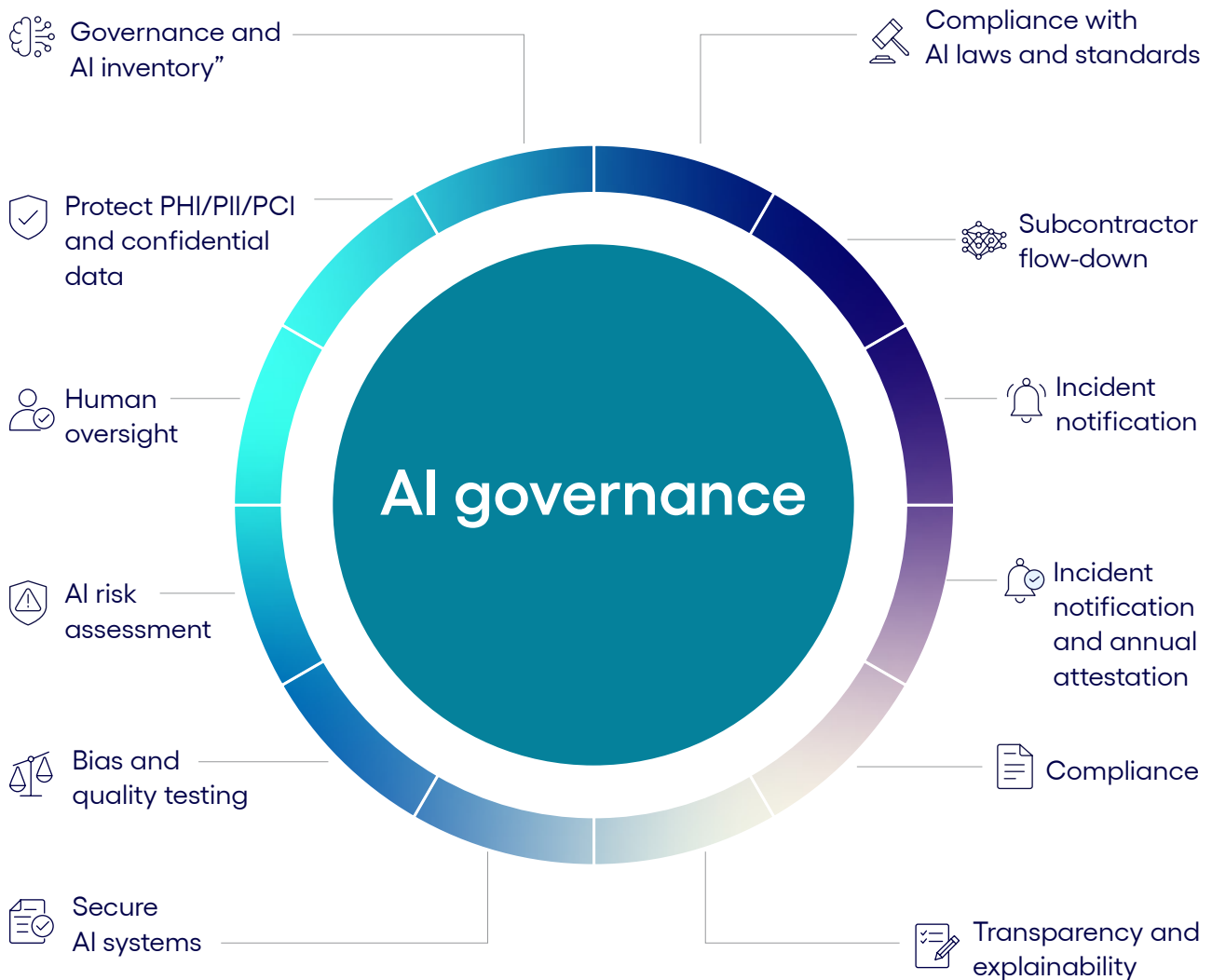
Sustainable and scalable

AI systems scale responsibly, with consideration of environmental and social impacts and continued alignment with ethical standards as systems evolve.



Vendor responsible AI requirements

Vendors that use AI in connection with Cognizant services must, at a minimum:



Governance and inventory

Maintain responsible AI governance, including a current inventory of AI tools used to deliver Cognizant services and clearly assigned roles and accountability for AI oversight.



Protect Cognizant and client data

Never enter Cognizant or Cognizant client PHI, PII, PCI or confidential information into public, consumer or otherwise unapproved AI tools. Use only approved, contractually permitted environments and apply privacy-by-design and data protection impact assessments.



Maintain human oversight

Maintain appropriate human oversight and governance over material AI-assisted decisions, particularly where AI outputs may impact healthcare operations, claims, eligibility determinations, utilization management, payment processing, member or patient communications, privacy rights, safety, regulatory compliance, or other healthcare or customer-facing outcomes.



Assess risk

Conduct AI risk and impact assessments before deployment and periodically thereafter, and document the results.



Test for bias and quality

Test AI systems for bias and validate datasets to promote fair and equitable outcomes.



Secure AI systems

Apply threat modeling, access controls, traceability, monitoring and incident-response mechanisms to AI systems that support Cognizant services.



Be transparent

Disclose to Cognizant the AI tools used in delivering services, provide explainability on request and label AI-generated content where required by law or contract.



Comply with applicable AI law

Consider and implement industry-recognized AI governance frameworks, standards and controls appropriate to the nature and risk profile of the AI solution, including, where applicable, ISO/IEC 42001 and the NIST AI Risk Management Framework.



Flow down to subcontractors

Impose equivalent responsible AI obligations on subcontractors, and downstream entities and monitor their compliance.



Notify Cognizant

Notify Cognizant in accordance with applicable contractual requirements regarding any AI-related incident, unauthorized entry of regulated data into an AI tool, model failure or other AI risk that materially impacts Cognizant services, data, security, regulatory compliance or contractual obligations.



Attest annually

Attest to responsible AI practices through the annual compliance questionnaire and provide supporting documentation upon request.

Reporting and questions

Suspected violations of responsible AI expectations may be reported—anononymously and without fear of retaliation—through the Cognizant Ethics and Compliance Helpline at 1-866-824-4897 or <https://www.cognizant.com/compliance-helpline>

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.



Cognizant (Nasdaq: CTSI) is an AI Builder and technology services provider, bridging the gap between AI investment and enterprise value by building full-stack AI solutions for our clients. Our deep industry, process and engineering expertise enables us to build an organization's unique context into technology systems that amplify human potential, drive tangible outcomes and keep global enterprises ahead in a fast-changing world. See how at cognizant.ai or @cognizant.

World Headquarters

300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Tel: +1 201 801 0233

European Headquarters

280 Bishopsgate
London
EC2M 4AG
England
Tel: +44 (0) 20 7297 7600

India Corporate office

Siruseri-Software Technology Park of India (STPI)
SDB Block – Ground floor North wing
Plot No H4, SIPCOT IT Park
Chengalpattu District
Chennai 603103, Tamil Nadu
Tel: 1800 208 6999

APAC Headquarters

1 Fusionopolis Link,
Level 5 NEXUS@One-North,
North Tower, Singapore 138542
Phone: + 65 6812 4000

© Copyright 2025–2027, Cognizant. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the express written permission of Cognizant. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.