CONE HEALTH	**Guideline:** ITS Third-Party Assurance Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 06/07/2024
	Effective Date: 06/07/2024	**Next Review Date:** 06/07/2025

INTENDED AUDIENCE:
Entire workforce

PROCEDURE:
In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), Cone Health is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), sensitive, and confidential data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this procedure is to define roles, responsibilities, and processes for assuring third party entities (e.g., vendors, consultants, contractors, service providers, etc.) comply with Cone Health's internal governance requirements for safeguarding covered information and applicable regulatory requirements.

Scope and Goals:
The scope of this procedure is to define the processes associated with the management of third-party relationships that Cone Health does business with. The goals of this procedure are as follows:

- Define contractual, service level agreement, or business associate agreement (BAA) requirements as they relate to the security and privacy of covered information.
- Define risk assessment requirements.

Responsibilities:
Chief Information Security Officer (CISO):
The CISO is responsible for, but not limited to. the following activities:

- Revisions, implementation, workforce education, interpretation, and enforcement of this procedure.
- Perform third party risk assessments on entities that will or could have access to covered information, prior to agreeing to signing any contractual agreements and engaging in any business activities that involve covered information.
- Work with the chief privacy officer to ensure that third parties who have access to covered information are being periodically audited to verify that the required security controls have been implemented.

Chief Privacy Officer:
The chief privacy officer is responsible for, but not limited to, the following activities:

- Ensure that all third-party relationships that will have access to covered information, specifically ePHI/PHI, have signed a BAA before Cone Health does any business with them.
- Annually review and update (if applicable) BAAs.

- Annually review third party relationships that have or could have access to ePHI/PHI to ensure a current BAA have been executed.

Information and Technology Services (ITS):
ITS is responsible for, but not limited to, the following activities:

- Assisting with the implementation and management of technical security controls related to third party relationships.

Management (individuals overseeing contractual relationship):
Management is responsible for, but not limited to, the following activities:

- Oversight and management of third-party relationships with support of the Procurement/Contracting office.
- Annually evaluate third party's performance against contract/service level agreements to ensure they are meeting agreed upon requirements.
- Conduct regular progress meetings to review reports, audit trails, security events, operational issues, failures, and disruptions, and investigate any issues till resolution.
- Hold periodic meetings with third parties to discuss service delivery and follow-up on any issues that might have been previously identified.
- Evaluate the potential impact of proposed service changes (to include system upgrades and patches if appropriate) to business processes prior to implementation.
- Document all third-party contractual exceptions and remediation activity.

Procurement/Contracting:
Procurement is responsible for, but not limited to, the following activities:

- Responsible for developing, disseminating, and annually reviewing and updating a list of current service providers and other third-party relationships (including a description of services provided).
- Periodically monitoring third party entities performance against what is required by their contract or agreement.
- Identifying third party relationships that are considered business associates and engage the CISO and chief privacy officer prior to signing any contractual agreements.
- Ensure that all third parties fully understand all contract/agreement language and requirements.

General Requirements:
Third party entities or BAs, will not be provided access (physical and logical) to Cone Health's covered information and systems until a risk assessment has been performed by the CISO and he/she can evaluate the entity's information security program to ensure the appropriate administrative, physical, and technical controls to safeguard covered information (see Third Party Risk Assessment below). Access provided is based on minimum necessary. The chief privacy officer will ensure that he/she has a signed BAA for those entities defined as BAs. BAs who do not sign a BAA or cannot comply with Cone Health's security/privacy requirements will not be allowed access to covered information or Cone Health's systems.

If a third-party entity is already in the process of contract negotiation and development, the provisions of the BAA (as defined by chief privacy officer and Legal Services) may be incorporated into the contract as an option (i.e., separate BAA not required).

Third Party Agreements/Contracts:
Agreements/contracts for third party entities that currently or could access/exchange covered information (i.e., physically and electronically) will contain the following content:

1. Name and contact information of the primary contact.
2. Date of establishment of agreement/contract.
3. General description of the type of service being provided.
4. Identification of the type of information that will be accessed, how it will be accessed (including specific functions, protocols, and ports that will be used) and if the information will be stored at a location owned/leased by the entity.
5. Service definitions, acceptable levels of service, and other aspects of services management. (e.g., monitoring, auditing, impacts to the organization's resilience, and change management).
6. Respective liabilities of the parties to the agreement.
7. Responsibilities with respect to legal matters and how it is determined that the legal requirements are met (e.g., data protection legislation) especially taking into account different national legal systems if the agreement involves cooperation with organizations in other countries.
8. Intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work (also, refer to the additional requirement in the Outsourced Software/Application Development section below).
9. Establish permitted uses and disclosures as applicable to the arrangement to include the third-party entity's employees and sub-contractor's requirement to manage access to covered information under the "minimum necessary" rule.
10. Name/signature of all individuals signing the agreement/contract.
11. Permitted and required uses and disclosures of covered information by the third-party entities.
12. Requirement that the third-party entity will not use or further disclose covered information other than as permitted or required by the contract or as required by law.
13. Requirement to implement appropriate safeguards to prevent unauthorized use or disclosure of covered information.
14. Requirement to conform to Cone Health's information security and privacy policies in the event of deficient documentation on the customer/vendor side.
15. Requirement for transmissions of covered information to be encrypted and conducted over encrypted channels.
16. Requirement for remote connections to utilize multi-factor authentication and encryption.
17. Requirement for implementation of information security, malicious software protections, access control, and information security awareness policies.
18. Requirement for preapproval from the CISO before using mobile or portable devices for the storage of covered information.
19. Participation in Cone Health's security training and awareness activities, unless it is determined the third-party entity has a sufficient security training and awareness program.

20. Requirement to report to Cone Health any use or disclosure of the information not authorized under their contract, including incidents that could constitute a breach of covered information as well as other suspected or known privacy and security incidents.
21. Requirement to disclose covered information as specified in its contract to satisfy Cone Health's obligation to individuals' requests for copies of their information (i.e., PHI/ePHI) as well as make available covered information (i.e., PHI/ePHI) for amendments (and incorporate any amendments, if required) and accountings.
22. Requirement to make available to Cone Health and/or HHS, its internal practices, books, and records relating to the use and disclosure of PHI/ePHI received from, or created, or received by the BA on behalf of Cone Health for purposes of HHS determining Cone Health's compliance with the HIPAA Privacy Rule.
23. Requirement to inform Cone Health's CISO within one business day if any transfers or terminations take place with third party personnel working at Cone Health's facilities that have organizational credentials, badges, or information system privileges.
24. Requirement to return all covered information it received from or created on behalf of Cone Health, upon termination of their agreement/contract. Include a statement that if the return of covered information is not feasible that they are required to return it when it is no longer needed or destroy the information and provide a detailed (i.e., itemized) document of destruction to Cone Health.
25. Requirement for subcontractors to agree to the same restrictions and conditions outlined in the agreement that the third-party entity has with Cone Health.
26. Requirement to undergo an annual security risk assessment by a third-party assessor and provide the results of the assessment or attestation letter to Cone Health.
27. Requirement to undergo an annual internal/external vulnerability assessment.
28. Requirement to coordinate, manage, and communicate changes to services provided to Cone Health through an approved change management process, providing allowance for Cone Health to evaluate proposed changes to identify the potential impacts before implementation.
29. Responsibilities for hardware and software installation, system maintenance, maintenance support, and/or spare parts for key information system components, configuration management, patch management, disaster recovery, data backup, etc. (i.e., ITS service providers).
30. Address service continuity requirements, including measures for availability, security, integrity, and reliability, including fallback arrangements for alternative technical services, such as information processing and communications facilities in accordance with the organization's business priorities.
31. Establishment of an escalation process for problem resolution.
32. Right of Cone Health to monitor and revoke any activity related to the Cone Health's services and assets.
33. Right to audit requirements outlined in the agreement/contract, to include contracting a third-party auditor to perform the audit.
34. Penalties exacted in the event of any failure of contractual obligations.
35. Authorization to terminate the contract if the entity or its subcontractors violate a material term of the contract.
36. Conditions surrounding the renegotiation/termination of agreements.
37. An indemnity clause.

38. Requirement and name of who is responsible for conducting background investigations for individuals that will be granted access to covered information or other sensitive organizational systems, providing results to Cone Health if requested, as well notification procedures to follow if screening has not been completed, or if the results give cause for doubt or concern, and the agreement with the third party clearly specifies all responsibilities and notification procedures for screening. (also refer to requirements in the Personnel Security Management procedure).
39. If applicable, restrictions on the physical locations used to store, process, or transmit covered information.
40. For relationships that involve electronic commerce transactions, the following terms must be defined:
    a. Determining the requirements for confidentiality, integrity, proof of dispatch, and receipt of key documents, and the non-repudiation of contracts (e.g., associated with tendering and contract processes).
    b. Authorization processes associated with who may set prices and issue or sign key trading documents.
    c. The level of confidence each party requires in each other's claimed identity (e.g., through authentication).
    d. Ensuring that all the parties involved are fully informed of their authorizations.
    e. The level of trust required for the integrity of advertised price lists.
    f. The degree of verification appropriate to check payment information supplied by a customer.
    g. Insurance requirements.
    h. Liability associated with any fraudulent transactions.
    i. Selecting the settlement form of payments to guard against fraud.

BAAs will include all mandatory language required by chief privacy officer and Legal Services.

Third Party Security Requirements:
Third party entities that access/exchange covered information will be required to maintain a formal information security program. Cone Health will ensure:

- Third party entities enforce minimum necessary when granting access to covered information.
- Third party entities limit their employees' access (both physical and logical access) to covered information for the duration of time needed.
- Transmission of covered information is encrypted.
- Third party entities are periodically made aware of their obligations.
- Third party entities address information security and other business considerations for continuity following a failure or disaster.
- The third-party entity is aware of Cone Health's information security policies/procedures that are applicable to the relationship.

Third Party Security Risk Assessment:
The evaluation of third-party risk will be in the form of a security risk assessment, conducted by the CISO. The security risk assessment will be performed in accordance with Cone Health's Information Security Risk Management procedure and utilizing the Third-Party Security Risk Assessment Questionnaire. Based on the results of the security risk assessment, Cone Health will determine

whether to engage in a business relationship with the third party. The security risk assessment will take the following into consideration:

1. The information asset(s) being accessed.
2. Type of access needed, such as:
   - Physical access (e.g., to offices, computer rooms, filing cabinets).
   - Logical access (e.g., to an organization's databases, information systems).
   - Network connectivity between the organization's and the external party's network(s) (e.g., permanent connection, remote access).
   - Whether access to covered information will only be onsite or if covered information will be stored off-site.
3. The value, sensitivity, and criticality of the information.
4. Accessibility needs of the third party.
5. Legal and regulatory requirements and other contractual obligations.

Third party entities will provide the following information in support of the security risk assessment:

1. Completed Third Party Security Risk Assessment Questionnaire.
2. Copies of their most recent information security risk assessment and vulnerability assessments.
3. Information security policies and procedures designed to detect, prevent, and mitigate risk.
4. Disaster recovery and business continuity plans,

Third party entities will not be allowed to access PHI/ePHI or organizational systems until:

- The CISO completes the security risk assessment and has analyzed the information to determine if risks are acceptable. Depending on the scope of the relationship, designated approving authority (see Information Security Risk Management procedure) review and approval may be required.
- The remediation of all risks (findings) that are determined to be unacceptable.
- Completion of background investigations for third party personnel who will be accessing covered information and/or information systems.
- Third party personnel have read the organization's information security policies and procedures and signed the Access Terms and Conditions agreement.

Independent Business Associate Risk Assessment:

Cone Health may utilize third party services to assist with third party risk assessments. If a third-party entity has had a risk assessment in the last year, they will be required to provide a copy of the assessment or a letter of attestation to Cone Health. If a risk assessment has not been performed or is over a year old, Cone Health will require the third-party entity to undergo an independent risk assessment, at their expense. Cone Health will determine the scope of this risk assessment.

For those third-party entities that are already doing business with Cone Health, they will be asked to provide a current information security risk assessment as soon as possible, otherwise face possible termination of their agreement/contract. The risk assessment must be performed by an independent assessor.

Outsourced Software/Application Development:
Outsourced software/application development will be in accordance with the following rules which will be addressed in the third-party agreements/contracts:

- Ownership of source code.
- Third parties will develop code based on industry secure coding best practices.
- New software or applications will undergo stress and security testing prior to being put into production to mitigate the risk of downtime, data breaches, and patient/client safety.
- Change control procedures will be used to track security flaws and the resulting resolution within the system.
- The development process is monitored by the organization and includes independent security and code reviews.

Documentation Retention:
Records related to security incidents, risk analysis, and breach decisions will be retained for a period of no less than 6 years from the date of the documentation.

Exception Management:
Exceptions to this procedure will be evaluated in accordance with Cone Health's Information Security Exception Management procedure.

Applicability:
All employees, volunteers, trainees, consultants, contractors, and other persons (i.e., workforce) whose conduct, in the performance of work for Cone Health, is under the direct control of Cone Health, whether or not they are compensated by Cone Health.

Compliance:
Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with Cone Health. Workforce members who fail to abide by requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.

Appendix 1

EXAMPLES OF BUSINESS ARRANGEMENTS THAT MAY INVOLVE DISCLOSURE OF PHI/ePHI (list is not all inclusive)	
Accrediting/Licensing Agencies (JCAHO) Accounting Consultants/Vendors Actuarial Consultants/Vendors Agents/Contractors Accessing PHI (Consultants) Application Service Providers (i.e., prescription mgmt.) Attorneys/Legal Counsel Auditors Benchmarking Organizations Benefit Management Organizations Claims Processing/Clearinghouse Agency Contracts Coding Vendor Contracts Collection Agency Contracts Computer Hardware Contracts Computer Software Contracts Consultants/Consulting Firms Data Analysis Consultants/Vendors Data Warehouse Contracts Emergency Physician Services Contracts Hospitalist Contracts Insurance Contracts (Coverage for Risk, Malpractice, etc.) Interpreter Services Contracts Information Technology Service Providers Legal Services Contracts Medical Staff Credentialing Software Contracts Microfilming Vendor Contracts Optical Disc Conversion Contracts	Pathology Services Contracts Paper Recycling Contracts Patient Satisfaction Survey Contracts Payer-Provider Contracts (Provider for Health Plan) Physician Billing Services Physician Contracts Practice Management Consultants/Vendors Professional Services Contracts Quality Assurance Consultants/Vendors Radiology Services Contracts Record Copying Service Vendor Contracts Record Storage Vendors Release of Information Service Vendor Contracts Repair Contractors of Devices Containing PHI Revenue Enhancement/DRG Optimization Contracts Risk Management Consulting Vendor Contracts Shared Service/Joint Venture Contracts with Other Healthcare Organizations Statement Outsource Vendors Telemedicine Program contracts Third Party Administrators Transcription Vendor Contracts Waste Disposal Contracts (Hauling, Shredding) Health Plan Relationships: • Pharmaceutical Benefits Management Contracts • Preauthorization Management Contracts • Case Management Contracts • Third Party Administrator (TPA) Contracts • Wellness Promotion Contracts

Appendix 1 Resource: HIPAA COW Business Associate Agreement Policy/Procedure, v5, 6/30/16

Appendix 2

EXAMPLES OF ARRANGEMENTS THAT ARE NOT BUSINESS ASSOCIATE RELATIONSHIPS AND DO NOT REQUIRE BA AGREEMENTS (list is not all-inclusive)	
Banks Processing Credit Card Payments Blood Bank/Red Cross (Provider) Clinics (Provider Relationships) Courier Services Delivering Specimens Device Manufacturers Require PHI to Produce Pacemakers, hearing aids, glasses, etc. (Treatment) Cleaning/Janitorial Services (Incidental exposure only) DME for Equipment for Treatment Purposes Educational/School Programs (Student Privacy Education Required as Workforce Member) Health Plans Contracting with Network Providers (Covered Entity to Covered Entity) Health Plans for Purposes of Payment Hospitals Housekeeping/Environmental Services (Incidental exposure only) Infusion Provider for Treatment Law Enforcement Agencies Members of an Affiliated Covered Entity Members of the Organization's Organized Health Care Arrangement (OHCA) Pharmacy (Healthcare Provider/Treatment) Providers (Involved in Care and Treatment of Patient)	Members of the Organization's Workforce Organ Procurement Organizations Nursing Homes Quality Improvement Organization –Agent of CMS (e.g., MetaStar) Rental Employee Agencies (No PHI Shared – Employees Need Privacy Training) Repair Contractors (Maintenance, Copy Machine, Plumbing, Electricity, etc. – No PHI involved) School Health Nurses Supply Services Support Services Agreements for Supplies/Tax Purposes Tissue Banks U.S. Post Office and Other Couriers Volunteers (Board Members, Ethics Committee Members, IRB Members, etc.)

Appendix 2 Resource: HIPAA COW Business Associate Agreement Policy/Procedure, v5, 6/30/16