CONFIDENTIALITY, PRIVACY, AND INFORMATION PROTECTION AGREEMENT

For the Cleveland County Veteran Coordinator
Accredited Through The American Legion

This Confidentiality, Privacy, and Information Protection Agreement ("Agreement") is adopted by **Cleveland County, Oklahoma, acting by and through its Board of County Commissioners** ("County"), and applies to the individual serving as the **Cleveland County Veteran Coordinator** ("Coordinator"), who is employed by the County and accredited through **The American Legion** to assist claimants in veterans' benefits matters. This Agreement establishes the confidentiality, privacy, and information-security obligations governing the Coordinator's handling of client information in the performance of official duties.

1. Purpose

The purpose of this Agreement is to protect the privacy rights of veterans, dependents, survivors, and other individuals served by the Cleveland County Veteran Coordinator office, and to establish minimum standards for the access to, use of, disclosure of, storage of, transmission of, and protection of confidential, sensitive, and protected information handled in the course of official duties.

2. Role of the Coordinator

A. The Cleveland County Veteran Coordinator is a County employee.

B. The same individual may be accredited through The American Legion to represent or assist claimants in veterans' benefits matters as allowed by applicable law and accreditation rules.

C. The Coordinator's dual role does not reduce, limit, or excuse the duty to protect client confidentiality.

D. This Agreement applies to all confidential information handled by the Coordinator and to County personnel who may have incidental or authorized access to such information in support, supervisory, legal, security, information-technology, or records-management functions.

3. Scope

This Agreement applies to all confidential, sensitive, or protected information handled in the course of the Coordinator's work, regardless of whether the information exists in paper, oral, electronic, visual, or other form.

4. Definitions

A. "Protected Health Information" or "PHI" means individually identifiable health information, to the extent protected by applicable law, including HIPAA where applicable.

B. "Personally Identifiable Information" or "PII" means information that identifies, relates to, describes, or is capable of being associated with a particular individual, including but not limited to name, date of birth, Social Security number, driver license number, passport number, military service information, claim numbers, VA file numbers, benefit identifiers, addresses, phone numbers, email addresses, and financial account information.

C. "Sensitive Personal Information" means PII, PHI, medical records, disability information, claim files, dependent information, financial records, military service records, and any other non-public data that could reasonably be used to identify, harm, embarrass, defraud, or compromise an individual.

D. "Confidential Information" means all non-public information received, accessed, created, stored, or transmitted in the course of the Coordinator's duties, including client files, claim documents, medical

evidence, legal documents, benefits records, passwords, security procedures, internal communications, and office records not intended for public disclosure.

E. “Client” means any veteran, dependent, survivor, claimant, or other individual assisted by the Coordinator office.

F. “Security Incident” means any attempted or actual unauthorized access, acquisition, use, disclosure, modification, destruction, loss, theft, or compromise of Confidential Information, whether intentional or accidental.

G. “Breach” means a Security Incident that triggers notice, mitigation, reporting, or remediation duties under applicable law, regulation, policy, or this Agreement.

5. General Confidentiality Obligations

A. Confidential Information shall be used solely for legitimate official purposes related to veterans’ representation, benefits assistance, claims development, appeals, office administration, legal compliance, and approved supervisory or operational support.

B. Access to Confidential Information shall be limited to those persons with a legitimate need to know in order to perform authorized duties.

C. Confidential Information shall not be sold, exploited, released, published, distributed, or otherwise disclosed except as authorized by the client, required by law, required for official claim processing, or expressly permitted under this Agreement.

D. The minimum necessary standard shall be applied whenever feasible.

E. Client information shall not be accessed out of curiosity or for any personal reason.

6. HIPAA, Medical Privacy, and Related Information

A. The County acknowledges that HIPAA applies only in circumstances where a person or entity is acting as a covered entity or business associate under applicable law.

B. To the extent HIPAA applies to any information or activity under this Agreement, the Coordinator and the County shall comply with applicable privacy, security, and breach-related requirements.

C. Even when HIPAA does not directly apply, medical, disability, and health-related information shall be protected using safeguards no less stringent than those set forth in this Agreement.

D. Nothing in this Agreement authorizes the disclosure of PHI or medical information except as permitted by law, by valid client authorization, or as necessary for legitimate benefits representation and related official functions.

7. Handling of PII and Sensitive Information

A. PII and Sensitive Personal Information shall be protected using reasonable and appropriate administrative, technical, and physical safeguards.

B. Such safeguards shall include, as applicable: secure workspaces; locked storage for paper records; strong passwords; multi-factor authentication where available; screen-lock and device-lock protections; controlled printing, copying, and scanning practices; shredding or secure destruction of paper records; restrictions on portable media and personal device use unless authorized; and secure transmission methods for sensitive information.

C. Personal email accounts, personal cloud storage, and unapproved messaging platforms shall not be used for transmitting or storing client information except where expressly authorized in writing and protected by reasonable safeguards.

8. Office-Specific Rules

A. Client files, intake forms, medical records, VA correspondence, supporting evidence, and related materials maintained in the Coordinator office shall be treated as Confidential Information.

B. County personnel who are not assigned a legitimate operational, legal, security, supervisory, technical support, or records-management role requiring access shall not review, handle, copy, scan, remove, or disclose client information.

C. Shared office equipment, including printers, scanners, copiers, computers, and network storage, shall be used in a manner reasonably designed to prevent unauthorized viewing, copying, retention, or disclosure of client information.

D. Paper files containing Confidential Information shall be secured in locked cabinets, desks, or offices when not in active use.

E. Computer screens displaying client information shall not be left visible to the public or unattended without appropriate screen-lock protections.

F. Client information shall not be discussed in hallways, waiting areas, elevators, break rooms, public meetings, or other places where unauthorized persons may overhear or observe the information.

9. Permitted Uses and Disclosures

A. To assist a client with benefits, claims, appeals, records requests, representation, or other authorized veterans' services matters.

B. To communicate with the United States Department of Veterans Affairs, Oklahoma Department of Veterans Affairs, medical providers, governmental agencies, courts, or other entities as authorized by the client or permitted by law.

C. For internal supervision, auditing, training, compliance, employment administration, and administrative functions on a need-to-know basis.

D. When required by law, subpoena, court order, public records ruling, or lawful investigative demand, provided that notice is given when legally permitted and reasonably practicable.

E. To report suspected abuse, neglect, criminal conduct, threats to safety, or other matters when disclosure is authorized or required by law.

10. Records Security, Retention, and Return

A. Records shall be maintained in a secure manner designed to prevent unauthorized access, loss, theft, or alteration.

B. Records shall be retained and destroyed in accordance with applicable law, records-retention schedules, and County policy.

C. Upon termination of employment, reassignment, separation, or conclusion of authorized access, the Coordinator shall promptly return all client files, keys, badges, credentials, devices, and other materials containing Confidential Information.

D. No copies shall be retained except as authorized by law or policy.

11. Security Incidents and Breach Response

A. Any known or reasonably suspected Security Incident or Breach shall be reported without unreasonable delay, and in no event later than two (2) business days after discovery, unless a shorter time is required by law.

B. The report shall include, to the extent known, the nature of the incident, the date or estimated date of occurrence and discovery, the categories of information involved, the number of affected individuals if known, and corrective actions taken or proposed.

C. The County and the Coordinator shall cooperate in investigation, containment, mitigation, required notifications, and remediation.

12. Public Records and Legal Process

A. Cleveland County may be subject to open records or public records requirements under Oklahoma law.

B. Confidential Information shall not be intentionally disclosed in response to a records request if an exemption, privilege, confidentiality law, privacy protection, or other lawful basis for withholding applies.

C. If a request, subpoena, or legal demand seeks client information, the matter shall be referred promptly to the appropriate County authority for legal review before disclosure, unless immediate disclosure is required by law.

13. Training and Compliance

A. The Coordinator shall comply with applicable County policies, records-handling requirements, accreditation duties, and privacy obligations relevant to the performance of official duties.

B. The County may require privacy, security, and confidentiality training reasonably related to the role.

C. Material noncompliance with this Agreement may result in discipline, restriction of access, reassignment, or other lawful action.

14. Term and Effect

This Agreement becomes effective upon the date of the last signature below and remains in effect unless superseded, amended, or terminated by County action. The confidentiality, records-protection, and incident-reporting obligations in this Agreement survive the Coordinator’s separation from employment or reassignment to the extent allowed by law.

15. Entire Agreement; Amendment

This Agreement constitutes the entire County agreement on the subject addressed herein for the Cleveland County Veteran Coordinator role and may be amended only in writing.

APPROVALS AND ACKNOWLEDGMENT

District 1 County Commissioner	By: _____ Name: _____ Title: Commissioner, District 1 Date: _____
District 2 County Commissioner	By: _____ Name: _____ Title: Commissioner, District 2 Date: _____
District 3 County Commissioner	By: _____ Name: _____ Title: Commissioner, District 3 Date: _____
County Attorney, Cleveland County, Oklahoma	By: _____ Name: _____ Title: Approved as to Form and Legality Date: _____
Acknowledged by Cleveland County Veteran Coordinator / American Legion Accredited Representative	Name: _____ Signature: _____ Date: _____

Note: This document is intended to establish County confidentiality and privacy obligations for the Cleveland County Veteran Coordinator role and to acknowledge that the Coordinator is accredited through The American Legion. It does not create The American Legion as a contracting party unless separately approved in writing.