Diligent Consulting
Data Use and Security Policy
Last revised 6/20/2026

1. Purpose

This Data Use and Security Policy ("Policy") establishes administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of Protected Health Information ("PHI") and client data handled by Diligent Consulting or its subcontractors (hereafter "Diligent Consulting").

This policy is an adjunct to the terms of the Work Services Agreement, as well as any Business Associate Agreement ("BAA") executed between Diligent Consulting and the Client ("Client"). Diligent Consulting will follow all applicable state regulations, contractual obligations, and provisions of the Health Insurance Portability and Accountability Act ("HIPAA").

This Policy shall be reviewed at least annually and updated as necessary to address regulatory, operational, or technological changes.

2. Scope

In this Policy, "**Data**" will refer to PHI governed by HIPAA Privacy and Security Rules, as well as non-PHI client data that are confidential or proprietary.

This policy applies to all consultants and subcontractors of Diligent Consulting, as well as all systems, devices, networks, cloud platforms, and applications used to store or process Data.

3. Training

All consultants and subcontractors with access to PHI or Client Data shall complete HIPAA Privacy and Security training through an accredited HIPAA and data security training program. This shall be completed at least annually and prior to being granted access to such information. Consultant shall maintain documentation of completed training and, upon reasonable request, provide confirmation of compliance to the Client in accordance with applicable BAA requirements.

4. Use of Data

Diligent Consulting will follow the Minimum Necessary Standard and agrees to use Data only as permitted or to the extent necessary to fulfill the duties and obligations under the Work Services Agreement and Statement of Work.

5. Data Safeguards

Diligent Consulting shall maintain commercially reasonable administrative, technical, and physical safeguards to prevent and mitigate accidental disclosure of Data. All consultants and subcontractors of Diligent Consulting will access data through a company email account that is secure and monitored.

Electronic Transmission of Data

Diligent Consulting will only receive Data via secure, HIPAA-compliant transfer mediums. Secure methods include encrypted email, HTTPS-based file transfers, and virtual private network (VPN) remote access. All data must be encrypted in transit and at rest.

When Data are received through an encrypted email, the user will delete the e-mail and empty the trash after the Data are downloaded and stored in a secure location. No Data will be retained in an email account.

Network Security

Diligent Consulting will not access or work with Data on a public or unsecured network.

Minimum Security Standards for Data Storage

The following options may be used to store electronic PHI:

- Cloud storage must utilize HIPAA-compliant services subject to a BAA, approved and maintained by Diligent Consulting. Examples may include enterprise-configured versions of Microsoft OneDrive or Google Workspace configured for HIPAA compliance.
- Only encrypted, company-approved removable media may be used to store Data.

In all scenarios, the following requirements must be met:

- Storage must have data encryption in transit and at rest (AES-256 at a minimum).
- Passwords must meet minimum complexity standards and shall not be shared between users.
- Multi-factor authentication is required for all company email accounts and systems containing Data.
- When PHI is stored on a physical media, the device must be stored in a locked cabinet when not in use.

No PHI may be created, received, maintained, accessed, or transmitted outside of the United States of America.

No Data may be saved or retained on an unsecured desktop, on an unsecured network, or on a physical media device lacking encryption and password protection.

Access to systems, accounts, and Data shall be promptly revoked upon termination of employment or subcontractor engagement, or upon completion of Services.

If statistical or mapping software requires data to be accessed on a local hard drive or storage device, Diligent Consulting will locally store only the minimal amount of Data required to perform the services in Statement of Work and will ensure the local storage location meets the requirements listed above.

Workstations and Devices

Personal workstations (laptop and desktop computers) must have password-protected access control and maintain current endpoint protection and security updates. Storage of Data on smartphones and tablets is prohibited.

Artificial Intelligence

The Consultant will not use artificial intelligence ("AI") tools, including generative AI platforms or machine learning systems, in connection with any data analysis, processing, storage, or reporting activities involving PHI. All analyses involving PHI will be conducted exclusively through secure, human-directed methods that comply with applicable privacy, security, and confidentiality requirements, including HIPAA. The Consultant will not input, upload, transmit, or expose PHI to any third-party AI system or service under any circumstances.

6. Data Ownership & Retention

Data ownership and retention vary by type of Data. Unless otherwise required by law, client agreement, IRB, or data use agreement, the following terms will apply:

Data	Owner	Diligent Consulting Retention
Any data or files related to a trauma designation or verification application or performance improvement activities	Client	Destroyed 60 days after payment of final invoice
Raw hospital data and raw trauma registry data	Client	2 years, then raw data destroyed
Raw data obtained by client from a governing entity (e.g., Hospital Discharge Data, state trauma registry data)	Client	2 years, then raw data destroyed
Transformed data (cleaned, recoded) manipulated by Diligent Consulting for analysis	Diligent Consulting	2 years with PHI, then scrubbed via the HIPAA Safe Harbor method to remove PHI. De-identified data retained up to 5 years then destroyed.
Programming code and analytic methodologies	Diligent Consulting or Subcontractor	Indefinitely
Templates, reports, or materials used for data reporting	Diligent Consulting or Subcontractor	Indefinitely

Data Destruction

Secure disposal methods of electronic Data shall be accomplished using hardware or software to overwrite physical storage media, rendering Data irretrievable. Secure deletion of cloud-based Data shall include permanent deletion from active systems and trash/recycle retention locations

where technically feasible, utilizing commercially reasonable certified destruction methods where applicable.

Documentation of Data Received and Destroyed
Data received and transmitted will be documented in a log maintained by Diligent Consulting. Retention periods, audits (if applicable), disposal date, and destruction method shall also be documented.

If the Work Services Agreement is terminated due to negligence on the part of Diligent Consulting, all files must be returned to Client and destroyed from Diligent Consulting files and servers.

7. Aggregate Reporting

Final reports will report Data only in aggregate format and will not disclose the identity of any individual patient. Population data will be suppressed for small counts (<5) when geographic or demographic identifiers could be used to potentially identify individuals.

8. Incident Response and Breach Notification

In the event of a breach, security incident, lost or stolen device, or any unauthorized or improper use or disclosure of Data, Diligent Consulting shall report such breach to the Client (or Subcontractor report to Diligent Consulting) without unreasonable delay and no later than five (5) business days after discovery. Notice of a breach or suspected breach shall include, at a minimum:

- Identification of the individual/company who is reasonably believed to have accessed, acquired, or disclosed data during the breach
- Date and time of the breach, if known
- Scope of the breach
- Description of the response to the breach

Diligent Consulting will investigate and document all incidents promptly to determine risk and PHI compromise. Diligent Consulting shall also reasonably cooperate with Client in investigating, mitigating, and responding to any security incident or breach involving Client Data or PHI. Where Diligent Consulting has knowledge of a material breach by a Subcontractor and judges it to be due to Subcontractor negligence, Diligent Consulting shall have the right to terminate the Work Services Agreement.

Data security services are provided by Secure Point Solutions.

9. Sanctions

Violations of this Policy may result in disciplinary action, termination of subcontractor engagement, or other corrective measures deemed appropriate by Diligent Consulting.