

LUMELIGHT HIPAA ADDENDUM

Version: HIPAA-2026-01

Effective Date: May 8, 2026

This HIPAA Addendum ("Addendum") forms part of and is incorporated into any applicable Lumelight Order Form or other ordering document referencing this Addendum between Compliance Holdings LLC d/b/a Lumelight ("Lumelight") and the applicable contracting party ("Client").

1. APPLICABILITY

This Addendum applies only to the extent Lumelight creates, receives, maintains, processes, or transmits Protected Health Information ("PHI") in connection with the Services.

Depending on Client's role under HIPAA and the nature of the Services:

- Client may act as a Covered Entity, Plan Sponsor, or Business Associate; and
- Lumelight may act as either:
 - a Business Associate; or
 - a Subcontractor to a Business Associate,

in each case as defined under HIPAA.

This Addendum shall apply only to the extent required by HIPAA and only with respect to PHI subject to HIPAA.

2. DEFINITIONS

- a. "**HIPAA**" means collectively the Health Insurance Portability and Accountability Act of 1996, the HITECH Act, and related regulations promulgated by the U.S. Department of Health and Human Services ("HHS").
- b. "**PHI**". "Protected Health Information" or "PHI" shall have the meaning assigned under HIPAA and shall be limited to information created, received, maintained, or transmitted by Lumelight on behalf of Client in connection with the Services.
- c. "**Security Incident**" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.
- d. "**Subcontractor**" shall have the meaning assigned under HIPAA.

3. PERMITTED USES AND DISCLOSURES

Lumelight may use and disclose PHI:

- a. to perform the Services;
- b. for proper management and administration of Lumelight's business;
- c. as required by law;
- d. to provide data aggregation services as permitted under HIPAA;
- e. to create de-identified information in accordance with HIPAA;
- f. to report violations of law; and
- g. for any other purpose permitted under HIPAA.

Lumelight shall limit uses and disclosures of PHI to the minimum necessary amount required to accomplish the intended purpose.

4. LUMELIGHT OBLIGATIONS

Lumelight shall:

- a. not use or disclose PHI except as permitted by this Addendum or required by law;
- b. implement appropriate administrative, technical, and physical safeguards to protect PHI;
- c. comply with applicable provisions of the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule;
- d. report to Client any Breach of Unsecured PHI or Security Incident without unreasonable delay following discovery;
- e. ensure that any Subcontractor receiving PHI agrees in writing to substantially similar restrictions and conditions;
- f. provide access, amendment, and accounting support to the extent required under HIPAA;
- g. cooperate with Client regarding HIPAA compliance obligations reasonably related to the Services; and
- h. mitigate harmful effects of any unauthorized use or disclosure of PHI to the extent practicable.

5. CLIENT OBLIGATIONS

Client shall:

- a. obtain all necessary authorizations, consents, and permissions relating to PHI;
- b. not request Lumelight to use or disclose PHI in any manner that would violate HIPAA;
- c. notify Lumelight of any applicable restrictions or limitations affecting PHI;
- d. remain solely responsible for plan administration decisions, benefit determinations, legal compliance obligations applicable to Client, and communications with individuals unless otherwise expressly agreed.

6. BREACH RESPONSE

In the event of a Breach of Unsecured PHI:

- a. Lumelight shall provide reasonably available information necessary for Client to satisfy applicable breach notification obligations;
- b. the parties shall reasonably cooperate in investigating and mitigating the incident; and
- c. unless otherwise agreed in writing, Client shall be responsible for determining whether notifications are legally required and for providing such notifications.

7. SUBCONTRACTORS

Lumelight may use Subcontractors in connection with the Services. Lumelight shall require any Subcontractor that creates, receives, maintains, or transmits PHI on Lumelight's behalf to agree to written obligations substantially similar to those contained in this Addendum.

8. DE-IDENTIFIED AND AGGREGATED DATA

Lumelight may de-identify PHI in accordance with HIPAA, create aggregated or anonymized data sets, and use such de-identified or aggregated data for any lawful business purpose. De-identified and aggregated data shall not constitute Protected Health Information and may be used by Lumelight for lawful business purposes.

9. TERM AND TERMINATION

This Addendum shall remain in effect for so long as Lumelight maintains PHI in connection with the Services.

Either party may terminate this Addendum for material breach if such breach remains uncured thirty (30) days after written notice.

Upon termination, Lumelight shall return or destroy PHI where required under HIPAA unless retention is legally required or operationally infeasible, in which case Lumelight shall continue protecting such PHI in accordance with this Addendum.

10. LIABILITY

Liability arising under this Addendum shall be governed by the limitation of liability provisions contained in the applicable Order Form and Service Terms unless otherwise expressly stated therein.

11. ORDER OF PRECEDENCE

If there is a conflict between this Addendum and the applicable Order Form or Service Terms regarding PHI or HIPAA compliance obligations, this Addendum shall control solely with respect to HIPAA-related matters.

12. ENTERPRISE / NEGOTIATED BAAS

If Client requires a separate negotiated business associate agreement, the parties may execute such agreement, which shall supersede this Addendum solely with respect to HIPAA-related matters addressed therein.

13. AMENDMENTS

Lumelight may publish updated versions of this Addendum from time to time. The version referenced in the applicable Order Form shall govern unless otherwise agreed in writing by the parties.

14. MISCELLANEOUS

This Addendum shall be interpreted in a manner consistent with HIPAA.

Any ambiguity shall be resolved in favor of a meaning that permits compliance with HIPAA.

If any provision of this Addendum is held invalid or unenforceable, the remaining provisions shall remain in full force and effect.