

# DOWNSTREAM BUSINESS ASSOCIATE AGREEMENT BETWEEN PODIUM AND SUBCONTRACTOR

This Downstream Business Associate Agreement (“**Downstream BAA**”) will be incorporated in the applicable Podium [Developer Terms](#) (the “**Developer Terms**”) for Developers in the Podium Developer Program (each a “**Subcontractor**”) that are business associates (as defined in HIPAA) or who process, store, or transfer Protected Health Information (“**PHI**”) (as defined in HIPAA) for use with certain products and services owned by Podium Corporation, Inc., a Delaware Corporation (“**Podium**”).

## Background

Pursuant to the parties’ agreement in the [Developer Terms](#), Subcontractor has agreed to perform certain services for or on behalf of Podium that may involve the creation, maintenance, use, transmission, or disclosure of protected health information on behalf of one or more of Podium’s Clients (each, a “**Covered Entity**” and collectively, “**Covered Entities**”) within the meaning of the Health Insurance Portability and Accountability Act of 1996 (“**HIPAA**”), the Health Information Technology for Economic and Clinical Health Act (“**HITECH**”), and their implementing regulations, 45 CFR Parts 160 and 164 (collectively the “**HIPAA Rules**”). Subcontractor is a subcontractor of Podium and is a Podium when Subcontractor requests, creates, receives, maintains, transmits, uses, or discloses (individually or collectively, “**Processes**”) PHI on behalf of Podium or one of Podium’s Clients (as defined in the [Developer Terms](#)). This **Downstream BAA** supplements the [Developer Terms](#) and is intended to and will be interpreted to satisfy the requirements for business associate agreements as set forth in the HIPAA Rules as they will be amended. Subcontractor understands and acknowledges that, as a business associate, Subcontractor is subject to certain HIPAA Rules, and that the violation of the HIPAA Rules carries significant administrative and criminal penalties as described in 45 CFR § 160.404 and 42 USC § 1320d-6.

In consideration of the mutual premises and covenants contained herein and in the [Developer Terms](#) and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Subcontractor and Podium agree as follows:

## 1. GENERAL PROVISIONS

**1.1. Defined Terms.** Capitalized terms used in this **Downstream BAA** without definition have the respective meanings assigned to such terms by the Administrative Simplification section of HITECH and HIPAA.

**1.2. Applicability.** Subcontractor acknowledges that (a) Podium is a Business Associate of its Covered Entities, and (b) Subcontractor is a downstream Business Associate of Podium under the [Developer Terms](#). This **Downstream BAA** relates to PHI that Subcontractor accesses or receives from Podium, a Covered Entity, or a third party on behalf of Podium in connection with this **Downstream BAA**.

**1.3. HIPAA Amendments.** The parties acknowledge and agree that HITECH and its implementing regulations impose requirements with respect to privacy, security, and breach notification applicable to Business Associates (collectively the “**HITECH BA Provisions**”). The HITECH BA Provisions and any other future amendments to HIPAA affecting business associate agreements are hereby incorporated by reference into this **Downstream BAA** as if set forth in this **Downstream BAA** in their entirety, effective on the later of the Effective Date or such subsequent date as may be specified by HIPAA.

**1.4. Regulatory References.** A reference in this **Downstream BAA** to a section in HIPAA means the section as it may be amended from time to time.

**1.5. Relationship of the Parties.** Subcontractor is and at all times during this **Downstream BAA** will be acting as an independent contractor to Podium, and not as Podium's agent. Podium will not have authority to control the method or manner in which Subcontractor performs its services on behalf of Podium, provided that Subcontractor complies with the terms of this **Downstream BAA** and the HIPAA Rules. Subcontractor will not have authority to bind Podium to any liability unless expressly authorized by Podium in writing, and Podium will not be liable for the acts or omissions of Subcontractor. Subcontractor will not represent itself as the agent of Podium. Nothing in this **Downstream BAA** will be deemed to establish an agency, partnership, joint venture, or other relationship except that of independently contracting entities.

**1.6. Rights to PHI.** Subcontractor acknowledges and agrees that neither it nor any of its employees, agents, consultants, or assigns will have any rights in any of the PHI or to Process the PHI in any form, including stripped or aggregated information or statistical information derived from or in connection with the PHI, except as expressly permitted in the [Developer Terms](#) and this **Downstream BAA**.

## 2. OBLIGATIONS OF SUBCONTRACTOR

**2.1. Subcontractor Responsibilities.** Subcontractor must fully comply with all relevant laws relating to the privacy or security of PHI applicable to Subcontractor, including but not limited to the HIPAA Rules as applicable to subcontractors. Subcontractor may not use or disclose PHI except as permitted by this **Downstream BAA** or as otherwise required by law. Subcontractor may only Process PHI as permitted or required under the [Developer Terms](#) (including this **Downstream BAA**) or as Required by Law but must not otherwise use, disclose, or Process PHI. Subcontractor must use appropriate safeguards to prevent the use or disclosure of PHI other than as permitted by this **Downstream BAA** or each Covered Entity **Downstream BAA**. To the extent applicable to business associates, Subcontractor will comply with the requirements in 45 CFR Part 164, Subpart C, including the use of administrative, physical, and technical safeguards to protect electronic protected health information. Subcontractor may not Process PHI in any manner that would constitute a violation of HIPAA if so used or disclosed by Podium or any Covered Entity except as set forth in Sections 2.1(b) and (c) of this **Downstream BAA**. To the extent Subcontractor carries out any of Podium's or a Covered Entity's obligations under the HIPAA Privacy Rule, Subcontractor must comply with the requirements of the HIPAA Privacy Rule that apply to Podium and Covered Entities in the performance of such obligations. To the extent Subcontractor is to carry out a Covered Entity's obligations under 45 CFR Part 164, Subpart E ("**HIPAA Privacy Rule**"), Subcontractor must comply with the requirements of the HIPAA Privacy Rule that apply to a Covered Entity in the performance of such obligations. Except as otherwise stated in this **Downstream BAA**, Subcontractor may not use or disclose PHI in a manner that would violate the HIPAA Rules if done by a Covered Entity. Under no circumstances will Subcontractor sell the PHI in violation of the HIPAA Rules Without limiting the generality of the foregoing, Subcontractor is permitted to use or disclose PHI as set forth below:

- (a) Subcontractor may use and disclose PHI to carry out Subcontractor's duties and obligations under the [Developer Terms](#) or under any agreement between Subcontractor and Podium or a Covered Entity;
- (b) Subcontractor may use PHI internally for Subcontractor's proper management and administrative services or to carry out its legal responsibilities;
- (c) To the extent required by the "minimum necessary" requirements of the HIPAA Rules, Subcontractor may only Process the minimum amount of PHI necessary to accomplish the purpose of the request, use, or disclosure. Subcontractor must comply with the minimum necessary guidance to be issued by the Secretary pursuant to HIPAA and, to the extent practicable, will not Process any Direct Identifiers (as defined in the limited data set standard of HIPAA).
- (d) Subcontractor may disclose PHI to a third party for Subcontractor's proper management and administration, provided that the disclosure is required by law or Subcontractor enters into a written agreement with the third party under which the third party agrees to (1) protect the confidentiality, security, and privacy of the PHI, (2) only use or further disclose the PHI as required by law or for the purpose for which the PHI was disclosed to the third party, and (3) notify Subcontractor of any instances of which the third party is aware in which the confidentiality of the PHI has been breached; and
- (e) Subcontractor agrees that none of the PHI it receives or its agents or subcontractors receive from Podium will be exported or stored (including temporary storage) outside of the United States.

**2.2. Safeguards.** Subcontractor must use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for

by this **Downstream BAA**. In addition, Subcontractor must implement Administrative Safeguards, Physical Safeguards, and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity, and Availability of Electronic Protected Health Information (“**EPHI**”) that it creates, receives, maintains, or transmits on behalf of Podium. Without limiting the foregoing, Subcontractor must comply with the HIPAA Security Rule and with all other applicable provisions of HIPAA with respect to EPHI.

**2.3. Mitigation.** Subcontractor must take reasonable steps to mitigate, to the extent practicable, any harmful effect (that is known to Subcontractor) of a use or disclosure of PHI by Subcontractor in violation of this **Downstream BAA** or HIPAA.

**2.4. Subcontractors.** Subcontractor may not subcontract any services that require it to disclose PHI that it has received from or created on behalf of Podium or any Covered Entities unless expressly authorized in the [Developer Terms](#) or this **Downstream BAA**. In the event Subcontractor is authorized to disclose such PHI, prior to any such permitted disclosure Subcontractor must enter into a written agreement meeting the requirements of 45 C.F.R. §§ 164.504(e) and 164.314(a)(2) with each Subcontractor (including, without limitation, a Subcontractor that is an agent under applicable law) that Processes PHI on behalf of Subcontractor. If Subcontractor is authorized to subcontract services, Subcontractor must ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of Subcontractor agree to the same restrictions, conditions, and requirements set forth in this **Downstream BAA** and the HIPAA Rules applicable to such subcontractors. Subcontractor may fulfill this requirement by executing a written agreement with the subcontractor incorporating the terms of this **Downstream BAA** and, to the extent necessary, otherwise complying with the requirements in 45 CFR §§ 164.308, 164.502, and 164.504. Subcontractor must ensure that the written agreement with each Subcontractor obligates the Subcontractor to comply with restrictions and conditions that are at least as restrictive as the restrictions and conditions that apply to Subcontractor under this **Downstream BAA**. In no event may Subcontractor, without Podium’s prior written approval, provide PHI to any employee or agent, including any Subcontractor, if such employee, agent, or Subcontractor receives, processes, or otherwise has access to the PHI outside of the United States.

**2.5. Reporting Requirements.** Subcontractor must immediately report to Podium any use or disclosure of PHI not permitted by this **Downstream BAA** or HIPAA of which Subcontractor becomes aware, including but not limited to (a) use or disclosure of PHI in violation of this **Downstream BAA** or HIPAA by Subcontractor or by a third party to which Subcontractor disclosed PHI, (b) breaches of unsecured PHI as required by 45 CFR § 164.410, and (c) security incidents as required by 45 CFR § 164.314. When Subcontractor reports a breach of Protected Health Information (whether secured or unsecured), the report must include the content required by 45 C.F.R. § 164.410 (collectively an “**Unauthorized Use or Disclosure**”). Subcontractor’s duty to report does not permit Subcontractor to notify those individuals whose PHI has been breached by Subcontractor without the express written permission of Podium to do so. All notifications to those individuals whose PHI has been breached must be made under the direction, review, and control of Podium. Subcontractor will not make any public disclosure, including to the media, of the foregoing without the approval of Podium, or in instances where Subcontractor is compelled by law or court order, without notifying Podium of such disclosure. The parties acknowledge that Subcontractor is periodically subject to attempted but unsuccessful attempts to access its information system (e.g., typical “pings” or port scans), but that such unsuccessful attempts are trivial, routine, and do not constitute a material threat to the security of PHI. The parties agree that further notice of such trivial but unsuccessful attempts will not be required unless expressly required by Podium.

**2.6. Cooperation with Podium.** Subcontractor will fully cooperate with Podium’s efforts to promptly investigate, mitigate, and notify third parties of breaches of unsecured protected health information or security incidents as required by the HIPAA Rules. Subcontractor will pay for or reimburse Podium for its expenses, costs, losses, payments, or damages resulting from any violation of the HIPAA Rules or breach of this **Downstream BAA** by Subcontractor or Subcontractor’s members, employees, agents, or subcontractors.

**2.7. Access to Information.** Within five (5) business days following Podium’s or a Covered Entity’s request, Subcontractor must make available to the related Covered Entity any PHI in Subcontractor’s control as necessary to enable the Covered Entity to satisfy its obligations to provide an individual with access to certain protected health information under 45 CFR § 164.524. If Subcontractor receives a request for access to PHI directly from an Individual, Subcontractor must forward such request to Podium within two (2) business days.

**2.8. Availability of PHI for Amendment.** Within ten (10) days following Podium’s or a Covered Entity’s request, make available to

Podium any PHI for amendment and incorporate any amendments to PHI as necessary to enable the Covered Entity to satisfy its obligations under 45 CFR § 164.526. If Subcontractor receives a request for an amendment to PHI directly from an Individual, Subcontractor must forward such request to Podium within two (2) business days.

**2.9. Accounting of Disclosures.** Within five (5) business days of written notice by Podium to Subcontractor that Podium has received a request for an accounting of disclosures of PHI (other than disclosures to which an exception to the accounting requirement applies), Subcontractor must deliver to Podium such Information in Subcontractor's possession that is required for Podium to make the accounting required by 45 C.F.R. § 164.528. If Subcontractor receives a request for an accounting directly from an Individual, Subcontractor must forward such request to Podium within five (5) business days. Subcontractor will have no responsibility for providing an accounting to the Individual. Such accounting is limited to disclosures of PHI that were made in the six (6) years prior to the request and must be provided for as long as Subcontractor maintains the PHI.

**2.10. Records; Availability of Books and Records.** Subcontractor must maintain information concerning Subcontractor's disclosures of PHI as required by 45 CFR § 164.528 and, within five (5) days following Podium's or a Covered Entity's request, make such information available to Podium and the Covered Entity as necessary to enable the Covered Entity to render an accounting of disclosures pursuant to 45 CFR § 164.528. In addition to any other such information, Subcontractor must document the following as to any impermissible disclosure: (i) the date of the disclosure; (ii) the name and address of the person or entity to whom the disclosure was made; (iii) a brief description of the protected health information disclosed; and (iv) a brief statement of the purpose of the disclosure. Subcontractor must promptly remedy any violation of any term of this **Downstream BAA** and must certify the same to Podium in writing. Subcontractor must make Subcontractor's internal practices, books, and records relating to the use and disclosure of PHI received from or created or received by Subcontractor on behalf of Podium or a Covered Entity, available to the Secretary for purposes of determining a Covered Entity's or Podium's compliance with HIPAA. In addition, if and to the extent requested by Podium or a Covered Entity, Subcontractor must provide to Podium and the Covered Entity such proof of Subcontractor's compliance with the requirements of this **Downstream BAA** as Podium or the Covered Entity will reasonably require.

**2.11. Indemnification.** Subcontractor agrees to indemnify, reimburse, defend, and hold harmless Podium for any costs, expenses, damages, fees, fines, settlements, judgments (including costs and attorney's fees), and other losses incurred as a result of a breach of this **Downstream BAA**, Unauthorized Use or Disclosure, Security Incident, or any acts or omissions of Subcontractor or Subcontractor's officers, members, employees, agents, or subcontractors arising out of the use and disclosure PHI or violation of the HIPAA Rules, or as a result of any negligence or willful misconduct by Subcontractor its agents or subcontractors, including, without limitation: fines or settlement amounts owed to a state or federal government agency; the cost of any notifications to Individuals or government agencies; credit monitoring for affected Individuals; or other mitigation steps taken by Podium to comply with HIPAA or state law.

### 3. ADDITIONAL RESTRICTIONS AND LIMITATIONS

**3.1. Permissions.** Podium will notify Subcontractor of any changes in, or revocation of any permission by an Individual to use or disclose the Individual's PHI, to the extent that any such change or revocation affects Subcontractor's use or disclosure of PHI. Subcontractor must comply with any such change or revocation.

**3.2. Restrictions & Confidential Communications.** Podium will notify Subcontractor of any request for a restriction on the use or disclosure of PHI or confidential communication to which Podium has agreed in accordance with 45 C.F.R. § 164.522, to the extent that such agreed-upon restriction or confidential communication request may affect Subcontractor's use or disclosure of PHI. Subcontractor must comply with any such agreed-upon restriction or confidential communication request.

**3.3. Covered Entities' Notices of Privacy Practices.** Podium will notify Subcontractor of any limitation in a Covered Entity's notice of privacy practices that limits Subcontractor's use or disclosure of PHI under this **Downstream BAA** Subcontractor must comply with such limitations.

### 4. TERMINATION OF THIS AGREEMENT

**4.1. Agreement Term.** The term of this **Downstream BAA** will commence on the Effective Date of the [Developer Terms](#) and will continue in full force and effect (and survive the expiration or earlier termination of this **Downstream BAA**) for so long as

Subcontractor maintains any PHI.

**4.2. Termination.** Podium may terminate this **Downstream BAA** upon ten (10) days prior notice if Podium determines that Subcontractor or any Subcontractor's subcontractor has violated the HIPAA Rules, a material term of this **Downstream BAA**, or otherwise engaged in conduct that may compromise the protected health information. Subcontractor will have the opportunity to cure the breach or violation within the 10-day notice period. If Subcontractor fails to cure the breach or violation within the 10-day notice period, Podium may declare this **Downstream BAA** and the [Developer Terms](#) terminated. Notwithstanding the foregoing, Podium may terminate this **Downstream BAA** immediately if Subcontractor or any subcontractor engages in any conduct that Podium reasonably believes may result in adverse action against Podium by any governmental agency or third party. Podium may terminate this **Downstream BAA** without cause upon thirty (30) days prior written notice to Subcontractor. This **Downstream BAA** will automatically terminate if the [Developer Terms](#) are terminated. Notwithstanding anything in the [Developer Terms](#) to the contrary, Podium will have the right to terminate the [Developer Terms](#) immediately, without penalty or liability, if Podium determines that Subcontractor's creation, maintenance, use, transmission, or disclosure of protected health information is a material purpose of the [Developer Terms](#) and this **Downstream BAA** is terminated for any reason.

**4.3. Obligations of Subcontractor upon Termination.** Upon earlier termination of the [Developer Terms](#) or of this **Downstream BAA**, Subcontractor agrees to return or destroy all PHI pursuant to 45 C.F.R. § 164.504(e) (2) (ii)(J), if it is feasible to do so. If it is not feasible for the Subcontractor to return or destroy said PHI, the Subcontractor will notify Podium in writing. This notification must include: (i) a statement that the Subcontractor has determined that it is not feasible to return or destroy the PHI in its possession, and (ii) the specific reasons for such determination. Subcontractor agrees to extend all protections, limitations, and restrictions contained in this **Downstream BAA** to Podium's use and/or disclosure of any PHI retained after the termination of this **Downstream BAA**, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the PHI infeasible. Upon request by Podium, Subcontractor will provide proof of compliance with this Section 4.3 to Podium in the form of an affidavit or other manner reasonably requested by Podium. Subcontractor's obligations under Section 2 will survive termination of this **Downstream BAA**.

## 5. MISCELLANEOUS

**5.1. Regulatory References.** A reference in this **Downstream BAA** to a section in the HIPAA Rules means the section as in effect or as amended.

**5.2. Amendments; Waiver.** This **Downstream BAA** may not be modified, nor may any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event may not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events. The Parties agree to take such action as is necessary to amend this **Downstream BAA** from time to time as is necessary for compliance with the requirements of the HIPAA and any other applicable law.

**5.3. Notices.** Any notices to be given hereunder to a Party must be made via U.S. Mail or express courier to such Party's address given below:

**If to Podium, to:**

Podium Corporation, Inc.  
1650 W. Digital Drive  
Lehi, UT 84043  
Attn: Legal Dept.

[legal@podium.com](mailto:legal@podium.com)

**If to Subcontractor, to:**

The email address used by Subcontractor to register for the Podium Developer Program.

**5.4. Interpretation.** Any ambiguity in this **Downstream BAA** will be interpreted to permit compliance with HIPAA.



**5.5. No Third-Party Beneficiaries.** Nothing express or implied in this **Downstream BAA** is intended to confer, nor may anything herein confer, upon any person other than the Parties and the respective successors or assigns of the parties, any rights, remedies, obligations, or liabilities whatsoever.

**5.6. Governing Law.** This **Downstream BAA** will be construed to comply with the requirements of the HIPAA Rules, and any ambiguity in this **Downstream BAA** will be interpreted to permit compliance with the HIPAA Rules. All other aspects of this **Downstream BAA** will be governed under the laws of Utah. Unless otherwise specified in the [Developer Terms](#), any action arising out of the breach or violation of his **Downstream BAA** will be pursued in the Relevant Jurisdiction, or the federal district court covering such county.

**5.7. Assignment/Subcontracting.** This **Downstream BAA** will inure to the benefit of and be binding upon the parties and their respective legal representatives, successors, and assigns. Subcontractor may assign or subcontract rights or obligations under this **Downstream BAA** to subcontractors or third parties without the express written consent of Podium provided that Subcontractor complies with Section 1.5. Podium may assign its rights and obligations under this **Downstream BAA** to any successor or affiliated entity.

**5.8. Cooperation.** The parties agree to cooperate with each other's efforts to comply with the requirements of the HIPAA Rules and other applicable laws; to assist each other in responding to and mitigating the effects of any breach of protected health information in violation of the HIPAA Rules or this **Downstream BAA**; and to assist the other party in responding to any investigation, complaint, or action by any government agency or third party relating to the performance of this **Downstream BAA**. In addition to any other cooperation reasonably requested by Podium, Subcontractor will make its officers, members, employees, agents, and subcontractors available without charge for interview or testimony.

**5.9. Insurance.** Unless waived in writing by Podium, Subcontractor will procure and maintain in effect during the term of this **Downstream BAA**: (1) general liability insurance coverage with minimum limits of \$3 million per occurrence and \$3 million aggregate; and (2) professional liability or errors and omissions insurance coverage within minimum limits of \$3 million per occurrence and \$3 million in aggregate, insuring against breaches of this **Downstream BAA**; (3) workers' compensation insurance coverage as required by law and employers liability in an amount not less than \$1 million, and (4) automobile liability insurance in the amount of \$1,000,000, if applicable. Upon request, Subcontractor will provide evidence of continuous coverage to Podium and no coverage required within this Section 5.9 will be voided or canceled without prior notice to Podium. Podium, its subsidiaries and affiliates, and its employees, trustees, directors, officers, subcontractors, agents, or other members of its workforce will be added as additional insureds on the liability policies required herein on a primary, non-contributory basis. If this agreement is supplemental documentation to a professional services or vendor agreement, then the greater of the insurance types and coverage requirements will take precedence to this clause. Upon Podium's request, Subcontractor will provide proof of such insurance to Podium.

**5.10. Relation to Developer Terms.** This **Downstream BAA** supplements the [Developer Terms](#). The terms and conditions of the [Developer Terms](#) will continue to apply to the extent not inconsistent with this **Downstream BAA**. If there is a conflict between this **Downstream BAA** and the [Developer Terms](#), this **Downstream BAA** will control. Notwithstanding any limitation on liability or other term in the [Developer Terms](#) to the contrary, Subcontractor's obligations pursuant to Sections 2(e) and 11 will apply in the event of any violation of the HIPAA Rules or breach of this **Downstream BAA** by Subcontractor or its members, employees, agents, or subcontractors.

**5.11. Entire Agreement.** This **Downstream BAA** contains the entire agreement between the parties as it relates to the use or disclosure of PHI and supersedes all prior discussions, negotiations, and services relating to the same to the extent such other prior communications are inconsistent with this **Downstream BAA**.

**5.12. Servability.** In case any provision in this **Downstream BAA** shall be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired thereby and such provision shall be ineffective only to the extent of such invalidity, illegality or unenforceability.

**5.13. Survival.** The terms in this **Downstream BAA** that must survive termination of this **Downstream BAA** to give them full effect will survive termination of this **Downstream BAA**, including but not limited to Sections 2, 3, 4.3, 5.6, 5.8, 5.9, and 5.10.

