

Business Associate Agreement

This Business Associate Agreement ("**Agreement**"), is made and entered into by and between _____ ("**Covered Entity**") and Webley, a division of Parus Holdings, Inc., ("**Service Provider**"), and (collectively the "**parties**"). The Underlying Contract(s) ("**Underlying Contract**") to which this Agreement applies include one or more agreements, written or oral, which the Parties have entered into, or may in the future enter into, under which Service Provider may be provided with, have access to, and/or create Protected Health Information. This Business Associate Agreement shall supplement and/or amend each of the Underlying Contracts only with respect to Service Provider's receipt, use, and creation of Protected Health Information pursuant to the Underlying Contracts to allow Covered Entity to comply with the requirements of the HIPAA Privacy and Security Rules.

NOW, THEREFORE, the parties, intending to be legally bound, agree as follows:

1. Current federal law, specifically Sections 1173 and 1175 of the Social Security Act (the Health Insurance Portability and Accountability Act of 1996) and 45 CFR Parts 160, 162, and 164 arising from that Act and commonly referenced as the Privacy & Security Rules (hereinafter referred to as "**HIPAA**"), and as further modified by the American Recovery and Reinvestment Act of 2009, establish enforceable privacy regulations governing the access, use, and disclosure of certain individually identifiable information. Covered Entity stores and transfers patient information in a manner that brings it within the scope of these laws. In accordance with HIPAA, Covered Entity is required to enter into an agreement with Service Provider regarding Service Provider's ability to access, use, and disclose information about Covered Entity's patients. Accordingly, Service Provider and Covered Entity agree to follow the terms and conditions set forth in this Agreement.
2. The parties acknowledge that federal and state laws relating to the security of electronic data and privacy of individual's health information are in a time of transition and that amendment of this Agreement may be required in order to ensure compliance with changes in the laws and clarifications of meaning provided by the governmental entities charged with enforcing the laws. The parties specifically agree to take such action as is necessary to implement the requirements of HIPAA and other applicable laws relating to the security and confidentiality of protected health information. In the event that counsel for Covered Entity determines that any term of this Agreement places Covered Entity, as a covered entity, at risk of violating such laws, then the applicable term(s) shall be subject to renegotiation and amendment. Upon request by Covered Entity, Service Provider agrees to enter promptly into negotiations regarding the terms of a written amendment to this Agreement to supplement and/or modify language as is required to comply with all applicable laws.
3. Service Provider acknowledges that Covered Entity collects confidential and other personal information concerning its patient's medical condition, care and treatment as contemplated in 45 C.F.R. § 160.103 (hereinafter referred to as "**Protected Health Information**"). Information deemed to be "**Protected Health Information**" includes information that directly identifies an individual or is of such a type or specificity that there is reasonable basis to believe the information could be used to identify an individual. Examples of

Protected Health Information include, but are not limited to, names, addresses, Social Security numbers, telephone numbers, electronic mail addresses, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, biometric identifiers, including finger and voice prints, full face photographic images, and any other unique identifying numbers, characteristics, or codes. Service Provider acknowledges that Covered Entity has a legal obligation to keep Protected Health Information confidential and that the unauthorized use and/or disclosure of Protected Health Information could irreparably damage Covered Entity and/or its patients. Due to its duties under the Underlying Contract, Service Provider and/or Service Provider's employees, agents, sub-contractors or representatives will or may gain access to Protected Health Information. Additionally, Service Provider acknowledges that it meets the definition of a "**Business Associate**" as defined in 45 CFR §160.103. Accordingly, Service Provider agrees to abide by the following requirements:

4. Service Provider and/or Service Provider's employees, agents, sub-contractors or representatives agree that they will abide by all applicable provisions of Sections 1173 and 1175 of the Social Security Act and any Rules or Regulations promulgated thereunder, including, but not limited to, 45 CFR Parts 160, 162, and 164, and further modified by the American Recovery and Reinvestment Act of 2009. Service Provider and/or Service Provider's employees, agents, sub-contractors or representatives further agree to comply with any amendments, revisions, and/or alterations of Sections 1173 and 1175 of the Social Security Act and 45 CFR Parts 160, 162, and 164. Additionally, Service Provider agrees to execute additional agreements as necessary to accommodate finalization and/or amendment of the above-cited law, rules or regulations.
5. Service Provider agrees that it will not access Protected Health Information other than as necessary to provide the services herein. Service Provider agrees that it will not otherwise use, disclose, remove, or otherwise alter any Protected Health Information maintained by Covered Entity without express written consent to do so.
6. Service Provider agrees that it will not use or disclose Protected Health Information other than as permitted by the Underlying Contract, this Agreement, or as required by law. This shall include holding Protected Health Information in strict confidence and not discussing, transmitting, or disclosing such Protected Health Information for any purposes other than as permitted by the contract and only after securing either proper authorization or consent as required by law, if such authorization or consent is necessary. Service Provider further agrees not to use or disclose Protected Health Information that would violate HIPAA regulations if Service Provider were a covered entity, even if the information was placed into Service Provider's possession through authorized means.
7. Service Provider acknowledges that Covered Entity is the rightful owner of all Protected Health Information provided to Service Provider by Covered Entity.
8. Covered Entity and Service Provider mutually acknowledge and agree that the permitted and required disclosures and uses of Protected Health Information under the Underlying Contract are limited to the uses and disclosures which are specifically enumerated in this Agreement.

9. Service Provider may make all uses of Protected Health Information necessary to perform its obligations under the Underlying Contract, provided such use comports with current laws, rules, and regulations. All other uses not authorized by this Agreement are prohibited.

10. Service Provider may disclose Protected Health Information for the purposes authorized by this Agreement:

(a) to its employees, subcontractors and agents, in accordance with the remaining terms of this Agreement, or

(b) as directed by Covered Entity, or

(c) as otherwise permitted by the terms of this Agreement including for its own proper management and administration, provided such disclosure comports with current laws, rules, regulations and advice and to fulfill any present or future legal responsibilities of Service Provider, provided that such uses are permitted under state and federal laws.

11. Service Provider may disclose the Protected Health Information in its possession to third parties for the purpose of its proper management and administration or to fulfill Service Provider's present or future legal responsibilities, provided that Service Provider represents to Covered Entity, in writing, that:

(a) the disclosures are required by law, as provided for in 45 C.F.R. § 164.502, or

(b) Service Provider has received from the third party written assurances regarding its confidential handling of such Protected Health Information as required under 45 C.F.R. § 164.504(e)(4).

12. Service Provider warrants and represents that any Protected Health Information requested pursuant to the Underlying Contract by Service Provider or Service Provider's employees, agents, sub-contractors or representatives shall be only the minimum information necessary to serve the intended purpose(s) of the Underlying Contract.

13. If Service Provider maintains patient information in a designated record set, Service Provider agrees to provide a patient the right to access, inspect, and copy their Protected Health Information in accordance with all provisions of 45 CFR §164.524.

14. If Service Provider maintains patient information in a designated record set, Service Provider agrees to provide a patient the right to amend their Protected Health Information in accordance with all provisions of 45 CFR §164.526.

15. Service Provider agrees to provide Covered Entity with an accounting of all disclosures of Protected Health Information in accordance with all provisions of 45 CFR §164.528. To the extent that Service Provider makes disclosures of Protected Health Information through an Electronic Health Record, Service Provider shall also record all disclosures for the purposes of

treatment, payment or health care operations, effective upon the compliance date applicable to Covered Entity for the recording of such disclosures.

16. Service Provider agrees to use appropriate safeguards to prevent the use or disclosure of Protected Health Information in any manner other than as provided for in this Agreement. Service Provider further agrees to take appropriate actions with each of Service Provider's employees, agents, contractors, sub-contractors and representatives who may have access to Protected Health Information to keep such information confidential and abide by the same restrictions, conditions and covenants contained in this agreement and further abide by all applicable laws, rules, regulations and advice.

17. Service Provider agrees to make its internal practices, books and records related to Protected Health Information available to the United States Department of Health and Human Services or its agents or designees as necessary for enforcement of the HIPAA regulations.

18. Service Provider agrees to provide Covered Entity access to all Protected Health Information in Service Provider's possession that was originally submitted to Service Provider by Covered Entity.

19. Service Provider agrees to maintain such policies, procedures and systems as may be necessary to prevent unauthorized parties from having access to, using, disclosing, processing, copying, modifying, corrupting, rendering unavailable, introducing computer code into or otherwise performing activities or operations upon or harmful to the privacy, availability, accessibility, integrity, structure, format or content of information maintained by Covered Entity resulting from Service Provider's access to such information. If Service Provider is allowed access to any Covered Entity computer system, Service Provider agrees to fully cooperate with Covered Entity to coordinate secure communications access to the computer system.

20. Service Provider agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic Protected Health Information that Service Provider creates, receives, maintains, or transmits on behalf of Covered Entity.

21. Service Provider agrees to maintain as secret any computer passwords or access codes, if applicable, that are assigned by Covered Entity. This includes not sharing passwords or other computer access codes with employees, agents, contractors, sub-contractors, representatives, associates and partners unless such employees, agents, contractors, sub-contractors, representatives, associates and partners have a specific need and right to know the computer passwords or access codes.

22. Service Provider agrees to report, in writing, to Covered Entity's designated Privacy Officer any use or disclosure of Protected Health Information that is not provided for in this Agreement, or any Security Incident, within five (5) days of the Service Provider's discovery of such unauthorized use and/or disclosure or Security Incident. Service Provider agrees to take all reasonable steps necessary to mitigate, to the greatest extent possible, any deleterious effects from any improper use and/or disclosure of Protected Health Information or any Security

Incident.

23. When patient-related information is in its possession, Service Provider agrees to comply with all applicable state laws and regulations relating to the confidentiality of such patient-related information including, without limitation, all such laws and regulations that impose more stringent requirements on Covered Entity and/or Service Provider than HIPAA.

24. With respect to electronic Protected Health Information, Service Provider agrees to take the following actions and be in compliance with the following requirements:

a) Service Provider agrees that it will implement policies and procedures to prevent, detect, contain, and correct security violations. Service Provider will perform and document in writing a risk analysis no less than every three (3) years to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information held by Covered Entity. Service Provider will conduct a risk analysis more frequently than every three (3) years if there is a significant change in the environment, including but not limited to: (a) introduction of new systems; (b) significant upgrades to existing systems; (c) retirement or disposal of systems; (d) physical relocation of IT assets; (e) introduction of new lines of business; and (f) reorganization of the Service Provider's management or business structure. The risk analysis must identify the systems which store, process, or transmit electronic Protected Health Information and identify the components of Service Provider's organization that handle electronic Protected Health Information, including the physical location of IT assets that contain electronic Protected Health Information. Service Provider must identify threats to the system as well as the probability that vulnerability will be exploited and an analysis of the controls that have been implemented or are planned for implementation. Service Provider shall identify corrective actions for any weaknesses identified by the risk analysis. The management of Service Provider shall be responsible for reviewing the risk analysis and approving the corrective action plan.

b) Service Provider will implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

c) Service Provider will apply appropriate sanctions against its workforce members who fail to comply with the security policies and procedures of Covered Entity and/or Service Provider.

d) Service Provider will implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

e) Service Provider will assign a member of its workforce to be responsible for the development and implementation of the security policies and procedures referenced herein.

f) Service Provider will implement policies and procedures to ensure that the members of its workforce are provided with appropriate levels of access to electronic Protected Health Information, including preventing those workforce members who do not need access to

electronic Protected Health Information from gaining access to electronic Protected Health Information. Service Provider's procedures for developing appropriate access for workforce members will include background investigations on personnel who have on-site and remote access to electronic Protected Health Information. Background investigations will be completed prior to personnel being allowed access to electronic Protected Health Information. Service Provider will identify and document which of its workforce positions it considers "high risk" and individuals in those "high risk" positions will be subject to a background check on a periodic basis. Service Provider will periodically review its list of "high risk" positions and modify the list as needed based on organizational and/or environmental changes.

g) Taking into consideration the specific needs and vulnerabilities of electronic Protected Health Information in Service Provider's possession, Service Provider will implement procedures regarding the approval process and/or supervision of those workforce members with access to electronic Protected Health Information. This will include implementing procedures to determine the appropriate level of access for the workforce member and procedures for terminating the workforce member's access.

h) Service Provider will conduct annual HIPAA (privacy and security) refresher training for its workforce members.

i) Service Provider will implement policies and procedures for authorizing access to electronic Protected Health Information that are consistent with the requirements of HIPAA.

j) If Service Provider is a health care clearinghouse and is also part of a larger organization, Service Provider will implement policies and procedures to protect electronic Protected Health Information of the clearinghouse from unauthorized access by the larger organization, including policies and procedures for granting, establishing, documenting, reviewing, and modifying access to electronic Protected Health Information.

k) Service Provider will implement a security awareness and training program for all members of its workforce (including management). The program will include, to a degree appropriate for Service Provider, periodic security updates; procedures for guarding against, detecting, and reporting malicious software; monitoring log-in attempts and reporting discrepancies; and creating, changing, and safeguarding passwords.

l) Service Provider will implement policies and procedures to address security incidents, including policies and procedures for identifying and responding to suspected or known security incidents, mitigating to the extent practicable, harmful effects of the security incidents, and documenting security incidents and their outcomes.

m) Service Provider will establish and implement as necessary policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic Protected Health Information, including procedures to create and maintain retrievable exact copies of electronic Protected Health Information, procedures to restore any loss of data, and procedures to enable continuation of critical business processes for the protections of the security of electronic

Protected Health Information while operating in emergency mode. This will include implementing procedures for periodic testing and revision of contingency plans and assessing the relative criticality of specific applications and data in support of other contingency plan components.

n) Service Provider will perform a periodic technical and nontechnical evaluation to establish the extent to which the Service Provider's security policies and procedures meet the requirements of HIPAA.

o) Service Provider will implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed. This may include establishing and implementing, as needed, procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and an emergency mode operations plan in the event of an emergency. It may also include implementing procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing. Service Provider will maintain records as appropriate to document repairs and modifications to the physical component of a facility which are related to security (for example, hardware, doors, and locks.)

p) Service Provider will implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic Protected Health Information.

q) Service Provider will implement physical safeguards for all workstations that access electronic Protected Health Information to restrict access to only those users who are authorized users.

r) Service Provider will implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic Protected Health Information into and out of a facility and the movement of these items within the facility, including, as appropriate, maintenance of a record of the movements of any hardware and media and the person responsible for the movement.

s) Service Provider will implement policies and procedures to address the final disposition of electronic Protected Health Information, and/or the hardware or electronic media on which it is stored, including, if needed, creating a retrievable copy of the electronic Protected Health Information prior to moving it.

t) Service Provider will implement procedures for the removal of electronic Protected Health Information from electronic media before the media is made available for re-use.

u) Service Provider will evaluate the need for electronic procedures that terminate an electronic session after a predetermined time of inactivity and will implement such procedures if appropriate.

v) Service Provider will evaluate the need for a mechanism to encrypt and decrypt electronic Protected Health Information and will implement such procedures if appropriate.

w) Service Provider will implement technical policies and procedures for electronic information systems that maintain electronic Protected Health Information to allow access only those persons or software programs that have been granted access rights.

x) Service Provider will assign a unique name and/or number for identifying and tracking user identity.

y) Service Provider will establish and implement procedures necessary for obtaining needed electronic Protected Health Information during an emergency.

z) Service Provider will implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic Protected Health Information.

aa) Service Provider will implement policies and procedures to protect electronic Protected Health Information from improper alteration or destruction. Service Provider will evaluate the need for an electronic mechanism to corroborate whether improper alteration or destruction of electronic Protected Health Information has occurred and will implement such mechanism if appropriate.

bb) Service Provider will implement procedures to verify that a person or entity seeking access to electronic Protected Health Information is the person or entity that they claim to be.

cc) Service Provider will implement technical security measures to guard against unauthorized access to electronic Protected Health Information that is being transmitted over an electronic communications network. Service Provider will evaluate the need for integrity controls and encryption and will implement such if appropriate.

dd) Service Provider will implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule. Service Provider will maintain the policies and procedures in written form, which may be in electronic format. Service Provider will maintain a written record, which may be in electronic format, for any action, activity or assessment that is required by the HIPAA Security Rule to be documented. Service Provider will retain this written documentation for a period of six (6) years from the date of its creation or the date where is last was in effect, whichever is later.

ee) Service Provider will make the documentation referenced in Section (dd) above available to those individuals who are responsible for implementing the procedures. Service Provider will periodically review the documentation and update as needed to address changes affecting the security of electronic Protected Health Information.

ff) If Service Provider is an independent contractor of Covered Entity, it shall notify Covered Entity of the discovery of a breach, or a suspected breach within the timeframe specified in Section 22 of this Agreement for reporting a Privacy or Security Incident. However, if Service Provider could be considered an agent of Covered Entity, Service Provider shall notify Covered Entity within two (2) business days of the discovery of a breach, or a suspected breach. The notification shall include as much information as is reasonably known about the events leading to the breach and shall include the identification of each individual whose unsecured Protected Health Information has been, or is reasonably believed to have been accessed, acquired, used or disclosed as soon as that information can be ascertained.

gg) Service Provider shall cooperate with Covered Entity to conduct an analysis of the risk of the potential harm to the individuals whose Protected Health Information has been compromised. This will include an analysis of the storage mechanisms for the Protected Health Information, the data elements that have been compromised, and all details regarding the circumstances by which the Protected Health Information came to be compromised. If Covered Entity determines that it is necessary to notify those individuals whose Protected Health Information has been compromised, Covered Entity shall make the decision as to whether it will send the notifications to the individuals or whether it will allow Service Provider to notify the individuals. If Covered Entity decides to send out the notifications, it will provide documentation of all reasonable costs associated with the notification, including but not limited to printing and postage costs, and Service Provider will promptly reimburse Covered Entity for the costs. Service Provider will also reimburse Covered Entity for all reasonable costs associated with operating a toll-free hotline for three (3) months that affected individuals may call with questions. Costs associated with the hotline include, but are not limited to, phone line charges and reasonable wage and benefit costs for individual(s) to answer calls to the hotline. The number of persons assigned to work the hotline will be based on the volume of calls received. If Covered Entity decides to allow Service Provider to send notifications directly to affected individuals, Service Provider will comply with the requirements put forth in the American Recovery and Reinvestment Act of 2009 for the contents of the letter. Service Provider will provide Covered Entity with an advance copy of the proposed letter for review and approval prior to sending to the affected individuals. Service Provider will remain responsible for the costs of printing and mailing letters to affected individuals. In the event that Covered Entity decides to allow Service Provider to host the required hotline for concerned individuals to call with concerns and questions, Service Provider shall be responsible for all costs associated with the hotline, including but not limited to phone lines and staffing. Service Provider agrees to maintain the availability of the hotline for three (3) months following the mailing of the notification letters to affected individuals.

25. Service Provider acknowledges that actual or threatened breach of this Agreement by Service Provider would cause serious and irreparable injury to Covered Entity and its patients. Therefore, in addition to any other remedies at law or in equity it may have, Covered Entity shall be entitled to equitable relief including without limitation, injunctive relief and specific performance. At any hearing for injunctive relief, Service Provider agrees that Covered Entity's burden of proof shall be by a preponderance of the evidence. As provided for under 45 CFR § 164.504(e)(2)(iii), Covered Entity may also immediately terminate the Underlying Contract and any other agreements existing between Service Provider and Covered Entity if Covered Entity

makes the determination that Service Provider has breached a material term of this Agreement. Alternatively, Covered Entity may choose to provide Service Provider with notice of the existence of an alleged material breach and afford Service Provider an opportunity to cure said alleged material breach. In the event Service Provider fails to cure said breach to the satisfaction of Covered Entity within five (5) days, Covered Entity may immediately thereafter terminate the Underlying Contract any other agreements existing between Service Provider and Covered Entity. Service Provider acknowledges that it shall be solely Covered Entity's option to seek injunctive relief, immediately terminate the Underlying Contract or any other agreements, or provide Service Provider an opportunity to cure an alleged material breach. The failure of Covered Entity to require performance by Service Provider of any provision of this Agreement shall in no way affect Covered Entity's right to enforce such provision, nor shall the waiver by Covered Entity of any breach of any provision of this Agreement be taken or held to be a waiver of any further breach of the same provision or any other provision.

26. Upon the termination of the Underlying Contract, Service Provider agrees to return or destroy all Protected Health Information pursuant to 45 C.F.R. § 164.504(e)(2)(ii)(I), if it is feasible to do so. Before doing so, Service Provider further agrees to recover any Protected Health Information in the possession of its subcontractors or agents. If it is not feasible for Service Provider to return or destroy said Protected Health Information, Service Provider will notify Covered Entity in writing. Said notification shall include a statement that Service Provider has determined that it is not feasible to return or destroy the Protected Health Information in its possession, and the specific reasons for such determination. Service Provider further agrees to extend any and all protections, limitations and restrictions contained in this Agreement to Service Provider's use and/or disclosure of any Protected Health Information retained after the termination of the Underlying Contract, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the Protected Health Information infeasible. If it is infeasible for Service Provider to obtain from a subcontractor or agent any Protected Health Information in the possession of the subcontractor or agent, Service Provider will provide a written explanation to Covered Entity and require the subcontractors and agents to agree to extend any and all protections, limitations and restrictions contained in this Agreement to the subcontractors' and/or agents' use and/or disclosure of any Protected Health Information retained after the termination of the Underlying Contract, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the Protected Health Information infeasible.

27. Service Provider agrees to indemnify, hold harmless, and defend Covered Entity and each of its employees, agents, attorneys, and officers from and against any and all claims, losses, damages, liabilities, costs, expenses, (including attorneys' fees) arising out of any claims, suits or demands resulting from Service Provider's use, misuse or disclosure of any Protected Health Information, be it related to the security, privacy or access of the Protected Health Information.

28. Service Provider agrees to maintain commercially reasonable insurance coverage to support its indemnification obligation.

29. Service Provider represents and warrants to Covered Entity that it will not enter into any agreement the execution and/or performance of which would violate or interfere with this

Agreement.

30. This Agreement shall not be construed against the party or parties preparing it. It shall be construed as if all the parties and each of them jointly prepared this Agreement, and resolved in favor of a meaning that permits Covered Entity to comply with HIPAA and the regulations promulgated pursuant thereto.

31. Nothing express or implied in this Agreement is intended to confer, nor shall 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.

IN WITNESS WHEREOF, the parties by their duly authorized representatives have executed this Agreement as of the date and year first above written. The person or persons signing and executing this contract on behalf of each party do hereby warrant and guarantee that he/she or they have been fully authorized by the respective party to execute this contract on behalf of the party and to validly and legally bind the party to all terms, performances and provisions set forth in the contract.

Webley, a division of Parus Holdings, Inc.

By: _____

Name/Title: _____

Date: _____

_____ **(Covered Entity)**

By: _____

Name/Title: _____

Date: _____