HABERSHAM COUNTY BOARD OF COMMISSIONERS

EXECUTIVE SUMMARY

SUBJECT: Business Associate Agreement related to HIPPA and Electronic Usage

DATE: January 29, 2019

(x) RECOMMENDATION
( ) POLICY DISCUSSION
( ) STATUS REPORT
( ) OTHER

BUDGET INFORMATION: N/A
ANNUAL-
CAPITAL-

COMMISSION ACTION REQUESTED ON: February 19, 2019

PURPOSE: To request Commission approval to adopt "Business Associate Agreement" as part of our annual contract agreement with Legacy Link.

BACKGROUND / HISTORY: The Business Associate Agreement is an updated version of the HIPPA document signed during contract renewal in past years. The agreement is to ensure staff compliance with HIPPA regulations as it relates to protecting client information when collecting and submitting electronic data via the Wellsky data base program.

FACTS AND ISSUES:
The Business Associate Agreement is a revised document to address compliance with HIPPA regulations related to collecting and transmitting private and confidential client information via electronic means.

OPTIONS:
1) Approve agreement to complete our annual contract with Legacy Link
2) Deny agreement approval to complete our annual contract with Legacy Link
3) Commission defined alternative

RECOMMENDED SAMPLE MOTION: I make a motion to approve the Business Associate Agreement.

DEPARTMENT:

Prepared by: Kathy Holcomb

Director _____Kathy Holcomb_____

ADMINISTRATIVE COMMENTS:_____

_____

_____

_____ **DATE:**_____

County Manager

Attachment A

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (hereinafter referred to as "Agreement") is made and entered into by and between The Legacy Link, Inc, Area Agency on Aging (hereinafter referred to as "AAA") and the ~~Habersham County Board of~~ Commissioners. (hereinafter referred to as "Contractor") as an attachment to Memorandum of Agreement between AAA and Contractor (hereinafter referred to as "Contract"). The effective date of this Agreement shall be the date the Contract referenced above is executed by Contractor.

WHEREAS, AAA is required by the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), to enter into a Business Associate Agreement with certain entities that provide functions, activities, or services involving the use of Protected Health Information, as defined by HIPAA;

WHEREAS, Contractor, under the Contract provides functions, activities, or services involving the use of Protected Health Information, as defined by HIPAA, and individually identifiable information ("PHI") protected by other state and federal law;

NOW, THEREFORE, for and in consideration of the mutual promises, covenants and agreements contained herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, AAA and Contractor (each individually a "Party" and collectively the "Parties") hereby agree as follows:

1. Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms have in HIPAA and in Title XIII of the American Recovery and Reinvestment Act of 2009 (the Health Information Technology for Economic and Clinical Health Act, or "HITECH"), and in the implementing regulations of HIPAA and HITECH. Implementing regulations are published as the Standards for Privacy and Security of Individually Identifiable Health Information in 45 C.F.R. Parts 160 and 164. Together, HIPAA, HITECH, and their implementing regulations are referred to in this Agreement as the "Privacy Rule and Security Rule." If the meaning of any defined term is changed by law or regulation, then this Agreement will be automatically modified to conform to such change. The term "NIST Baseline Controls" means the baseline controls set forth in National Institute of Standards and Technology (NIST) SP 800-53 established for "moderate impact" information.

2. Except as limited in this Agreement, Contractor may use or disclose PHI only to the extent necessary to meet its responsibilities as set forth in the Contract provided that such use or disclosure would not violate the Privacy Rule or the Security Rule, if done by AAA. Furthermore, except as otherwise limited in this Agreement, Contractor may:

A. Use PHI for internal quality control and auditing purposes.

B. Use or disclose PHI as Required by Law.

C. After providing written notification to AAA , use PHI to make a report to a health oversight agency authorized by law to investigate AAA(or otherwise oversee the conduct or conditions of the AAA) about any AAA conduct that Contractor in good faith believes to be unlawful as permitted by 45 C.F.R. 164.502(j)(1). Notwithstanding the foregoing, Contractor shall not be required to provide prior written notice to AAA Privacy Officer if Contractor is provided

written instruction otherwise by the health oversight agency authorized by law to investigate AAA.

D. Use and disclose PHI to consult with an attorney for purposes of determining Contractor's legal options with regard to reporting conduct by AAA that Contractor in good faith believes to be unlawful, as permitted by 45 C.F.R. 164.502(j)(1).

3. Contractor warrants that only individuals designated by title or name on **Attachments A-1** and **A-2** will request PHI from AAA or access AAA PHI in order to perform the services of the Contract, and these individuals will only request the minimum necessary amount of information necessary in order to perform the services.

4. Contractor warrants that the individuals listed by title on **Attachment A-1** require access to PHI in order to perform services under the Contract. Contractor agrees to send updates to **Attachment A-1** whenever necessary. Uses or disclosures of PHI by individuals not described on **Attachment A-1** are impermissible.

5. Contractor warrants that the individuals listed by name on **Attachment A-2** require access to a DHS information system in order to perform services under the Contract. Contractor agrees to notify the HCBS Program Manager and the MIS Director named on **Attachment A-2** immediately, but at least within twenty-four (24) hours, of any change in the need for DHS information system access by any individual listed on **Attachment A-2**. Any failure to report a change within the twenty-four (24) hour time period will be considered a security incident and may be reported to Contractor's Privacy and Security Officer, Information Security Officer and the Georgia Technology Authority for proper handling and sanctions.

6. Contractor agrees that it is a Business Associate to AAA as a result of the Contract, and warrants to AAA that it complies with the Privacy Rule and Security Rule requirements that apply to Business Associates and will continue to comply with these requirements. Contractor further warrants to AAA that it maintains and follows written policies and procedures to achieve and maintain compliance with the HIPAA Privacy and Security Rules and updates such policies and procedures as necessary in order to comply with the HIPAA Privacy and Security Rules that apply to Business Associates. These policies and procedures shall be provided to AAA upon request.

7. The Parties agree that a copy of all communications related to compliance with this Agreement will be forwarded to the following Privacy and Security Contacts:

A. At AAA: Christine Bittle
HCBS Program Manager; Community Programs Director
cjbittle@legacylink.org
678-677-8474

Dianne Dodgins, Health Programs Director at Legacy Link
dddodgins@legacylink.org
770-538-2669

B. At Contractor: _____
_____

8. Contractor agrees that it will:

A. Not request, create, receive, use or disclose PHI other than as permitted or required by this Agreement, the Contract, or as required by law.

B. Establish, maintain and use appropriate administrative, physical and technical safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement or the Contract. Such safeguards must include all NIST Baseline Controls, unless DHS has agreed in writing that the control is not appropriate or applicable.

C. Implement and use administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of AAA/DHS. Such safeguards must include all NIST Baseline Controls, unless DHS has agreed in writing that the control is not appropriate or applicable.

D. In addition to the safeguards described above, include access controls that restrict access to PHI to the individuals listed on **A-1** and **A-2**, as amended from time to time, and shall implement encryption of all electronic PHI during transmission and at rest.

E. Upon DHS' reasonable request, but no more frequently than annually, obtain an independent assessment of Contractor's implementation of the NIST Baseline Controls and the additional safeguards required by this Agreement with respect to DHS PHI, provide the results of such assessments to DHS, and ensure that corrective actions identified during the independent assessment are implemented.

F. Mitigate, to the extent practicable, any harmful effect that may be known to Contractor from a use or disclosure of PHI by Contractor in violation of the requirements of this Agreement, the Contract or applicable regulations. Contractor shall bear the costs of mitigation, which shall include the reasonable costs of credit monitoring or credit restoration when the use or disclosure results in exposure of information commonly used in identity theft.

G. Ensure that its agents or subcontractors to whom it provides PHI are contractually obligated to comply with at least the same obligations that apply to Contractor under this Agreement, and ensure that its agents or subcontractors comply with the conditions, restrictions, prohibitions and other limitations regarding the request for, creation, receipt, use or disclosure of PHI, that are applicable to Contractor under this Agreement and the Contract.

H. Except for "Non-Reportable Incidents," report to AAA any use or disclosure of PHI that is not provided for by this Agreement or the Contract of which it becomes aware. Non-Reportable Incidents are limited to the following:

i. the unintentional acquisition, access, or use of PHI by a workforce member of Contractor acting under the authority of Contractor, so long as the PHI is not further acquired, accessed, used or disclosed in an impermissible manner;

ii. the inadvertent disclosure of PHI from a person designated in **A-1** or **A-2** as authorized to access DHS PHI to a workforce member of Contractor who is not designated in **A-**

1 or **A-2**, but is authorized to access other Protected Health Information maintained by Contractor, so long as the information is not further acquired, accessed, used or disclosed in an impermissible manner.

I. Make an initial report to AAA in writing in such form as AAA may require within three (3) business days after Contractor (or any subcontractor) becomes aware of the unauthorized use or disclosure. This report will require Contractor to identify the following:

i. The nature of the impermissible use or disclosure (the "incident"), which will include a brief description of what happened, including the date it occurred and the date Contractor discovered the incident;

ii. The PHI involved in the impermissible use or disclosure, such as whether the full name, social security number, date of birth, home address, account number or other information were involved;

iii. Who (by title, access permission level and employer) made the impermissible use or disclosure and who received the PHI as a result;

iv. What corrective or investigational action Contractor took or will take to prevent further impermissible uses or disclosures, to mitigate harmful effects, and to prevent against any further incidents;

v. What steps individuals who may have been harmed by the incident might take to protect themselves; and

vi. Whether Contractor believes that the impermissible use or disclosure constitutes a Breach of Unsecured PHI.

Upon request by the AAA HCBS Program Manager and HIPAA Compliance Officer, Contractor agrees to make a complete report to the AAA in writing within two (2) weeks of the initial report that includes a root cause analysis and a proposed corrective action plan. Upon approval of a corrective action plan by the AAA, Contractor agrees to implement the corrective action plan and provide proof of implementation to the AAA within five (5) business days of AAA's request for proof of implementation.

J. Report to the AAA HCBS Program Manager and HIPAA Compliance Officer any successful unauthorized access, modification, or destruction of PHI or interference with system operations in Contractor's information systems as soon as practicable but in no event later than three (3) business days of discovery. If such a security incident resulted in a use or disclosure of PHI not permitted by this Agreement, Contractor shall also make a report of the impermissible use or disclosure as described above. Contractor agrees to make a complete report to the AAA in writing within two weeks of the initial report that includes a root cause analysis and, if appropriate, a proposed corrective action plan designed to protect PHI from similar security incidents in the future. Upon AAA's approval of Contractor's corrective action plan, Contractor agrees to implement the corrective action plan and provide proof of implementation to the AAA.

K. Upon AAA's reasonable request and not more frequently than once per quarter, report to the AAA HIPAA Compliance Officer any (A) attempted (but unsuccessful) unauthorized access, use, disclosure, modification, or destruction of PHI or (B) attempted (but unsuccessful) interference with system operations in Contractor's information systems. Contractor does not need to report trivial incidents that occur on a daily basis, such as scans, "pings," or other routine attempts that do not penetrate computer networks or servers or result in interference with system operations.

L. Cooperate with AAA and provide assistance necessary for AAA to determine whether a Breach of Unsecured PHI has occurred, and whether notification of the Breach is legally required or otherwise appropriate. Contractor agrees to assist AAA in its efforts to comply with the HIPAA Privacy and Security Rules, as amended from time to time. To that end, the Contractor will abide by any requirements mandated by the HIPAA Privacy and Security Rules or any other applicable laws in the course of this Contract. Contractor warrants that it will cooperate with AAA, including cooperation with AAA privacy officials and other compliance officers required by the HIPAA Privacy and Security Rules and all implementing regulations, in the course of performance of this Contract so that both Parties will be in compliance with HIPAA.

M. If AAA determines that a Breach of Unsecured PHI has occurred as a result of Contractor's impermissible use or disclosure of PHI or failure to comply with obligations set forth in this Agreement or in the Privacy or Security Rules, provide all notifications to Individuals, HHS and/or the media, on behalf of AAA, after the notifications are approved by the AAA. Contractor shall provide these notifications in accordance with the security breach notification requirements set forth in 42 U.S.C. §17932 and 45 C.F.R. Parts 160 & 164 subparts A, D & E as of their respective Compliance Dates, and shall pay for the reasonable and actual costs associated with such notifications.

In the event that AAA determines a Breach has occurred, without unreasonable delay, and in any event no later than thirty (30) calendar days after Discovery, Contractor shall provide the AAA HIPAA Compliance Officer a list of Individuals and a copy of the template notification letter to be sent to Individuals. Contractor shall begin the notification process only after obtaining AAA's approval of the notification letter.

N. Make any amendment(s) to PHI in a Designated Record Set that DHS directs or agrees to pursuant to 45 CFR 164.526 within five (5) business days after request of AAA. Contractor also agrees to provide AAA with written confirmation of the amendment in such format and within such time as AAA may require.

O. In order to meet the requirements under 45 CFR 164.524, regarding an individual's right of access, within five (5) business days following AAA's request, or as otherwise required by state or federal law or regulation, or by another time as may be agreed upon in writing by the AAA, provide AAA access to the PHI in an individual's Designated Record Set. However, if requested by AAA, Contractor shall provide access to the PHI in a Designated Record Set directly to the individual to whom such information relates.

P. Give the Secretary of the U.S. Department of Health and Human Services (the "Secretary") or the Secretary's designees access to Contractor's books and records and policies, practices or procedures relating to the use and disclosure of PHI for or on behalf of DHS within five (5) business days after the Secretary or the Secretary's designees request such access or

otherwise as the Secretary or the Secretary's designees may require. Contractor also agrees to make such information available for review, inspection and copying by the Secretary or the Secretary's designees during normal business hours at the location or locations where such information is maintained or to otherwise provide such information to the Secretary or the Secretary's designees in such form, format or manner as the Secretary or the Secretary's designees may require.

Q. Document all disclosures of PHI and information related to such disclosures as would be required for AAA to respond to a request by an Individual or by the Secretary for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. By no later than five (5) business days of receipt of a written request from AAA, or as otherwise required by state or federal law or regulation, or by another time as may be agreed upon in writing by the AAA HIPAA Compliance Officer, Contractor shall provide an accounting of disclosures of PHI regarding an Individual to AAA. If requested by AAA, Contractor shall provide an accounting of disclosures directly to the individual. Contractor shall maintain a record of any accounting made directly to an individual at the individual's request and shall provide such record to the AAA upon request.

R. Work in good faith with AAA to promptly resolve any dispute, controversy or claim arising out of or relating to a violation of the HIPAA Privacy and Security Rules or Breach that arises from the conduct or omission of Business Associate or its employee(s), agent(s) or subcontractor(s). Business Associate acknowledges that such a violation of the HIPAA Privacy and Security Rules or breach of this Agreement may result in financial harm to AAA, including, but not limited to, damages, fines, civil penalties and reasonable attorneys' fees imposed on AAA as a result of such conduct or omission. Business Associate agrees to act in good faith to mitigate such financial harm to AAA, including, but not limited to, pursuing or assisting AAA in its pursuit of any financial recovery available through insurance or other financial coverage maintained by the Department of Administrative Services or any successor entity, pursuing any financial recovery available through Business Associate's contracts with its agents or subcontractors as applicable, or taking such other action as determined reasonable by AAA and the Business Associate taking into consideration State budgetary requirements and restrictions.

9. AAA agrees that it will:

A. Notify Contractor of any new limitation in AAA's Notice of Privacy Practices in accordance with the provisions of the Privacy Rule if, and to the extent that, AAA determines in the exercise of its sole discretion that such limitation will affect Contractor's use or disclosure of PHI.

B. Notify Contractor of any change in, or revocation of, authorization by an Individual for AAA to use or disclose PHI to the extent that AAA determines in the exercise of its sole discretion that such change or revocation will affect Contractor's use or disclosure of PHI.

C. Notify Contractor of any restriction regarding its use or disclosure of PHI that AAA has agreed to in accordance with the Privacy Rule if, and to the extent that, AAA determines in the exercise of its sole discretion that such restriction will affect Contractor's use or disclosure of PHI.

D. Prior to agreeing to any changes in or revocation of permission by an Individual, or any restriction, to use or disclose PHI, AAA agrees to contact Contractor to determine feasibility of compliance. Following the receipt by AAA of a written cost estimate, AAA agrees to assume all costs incurred by Contractor in compliance with such special requests.

10. The **Term of this Agreement** shall be effective on the Effective Date and shall terminate when all of the PHI provided by AAA to Contractor, or created or received by Contractor on behalf of AAA, is destroyed or returned to AAA, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this section.

A. Termination for Cause. Upon AAA's knowledge of a material breach of this Agreement by Contractor, AAA shall either:

i. Provide an opportunity for Contractor to cure the breach of Agreement within a reasonable period of time, which shall be within thirty (30) calendar days after receiving written notification of the breach by DHS;

ii. If Contractor fails to cure the breach of Agreement, terminate the Contract upon thirty (30) calendar days' notice; or

iii. If neither termination nor cure is feasible, AAA shall report the breach of Agreement to the Secretary of the Department of Health and Human Services.

B. Effect of Termination.

i. Upon termination of this Agreement, for any reason, AAA and Contractor shall determine whether return of PHI is feasible. If return of the PHI is not feasible, Contractor agrees to continue to extend the protections of this Agreement to the PHI for so long as the Contractor maintains the PHI and shall limit the use and disclosure of the PHI to those purposes that made return or destruction of the PHI infeasible. If at any time it becomes feasible to return or destroy any such PHI maintained pursuant to this paragraph, Contractor must notify AAA and obtain instructions from AAA for either the return or destruction of the PHI.

ii. Contractor agrees that it will limit its further use or disclosure of PHI only to those purposes AAA may, in the exercise of its sole discretion, deem to be in the public interest or necessary for the protection of such PHI, and will take such additional actions as AAA may require for the protection of patient privacy and the safeguarding, security and protection of such PHI.

iii. This Effect of Termination section survives the termination of the Agreement.

11. Interpretation. Any ambiguity in this Agreement shall be resolved to permit AAA to comply with applicable laws, rules and regulations, the HIPAA Privacy Rule, the HIPAA Security Rule and any rules, regulations, requirements, rulings, interpretations, procedures or other actions related thereto that are promulgated, issued or taken by or on behalf of the Secretary; provided that applicable laws, rules and regulations and the laws of the State of Georgia shall supersede the Privacy Rule if, and to the extent that, they impose additional requirements, have requirements that are more stringent than or have been interpreted to provide greater protection of patient privacy or the security or safeguarding of PHI than those of the HIPAA Privacy Rule.

12. **No Third Party Beneficiaries.** 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.

13. **All other terms and conditions contained in the Contract and any amendment thereto, not amended by this Agreement, shall remain in full force and effect.**

IN WITNESS WHEREOF, Contractor, through its authorized officer and agent, has caused this Agreement to be executed on its behalf as of the date indicated.

Contractor Name: Habersham County Board of Commissioners

BY: _____ _____
SIGNATURE DATE

_____

_____
TITLE*

* Must be President, Vice President, CEO or Other Officer Authorized to Execute on Behalf of and Bind the Entity to a Contract

ATTACHMENT A-1

List of Individuals Permitted to Receive, Use and Disclose DHS PHI

The following Position Titles, as employees and/or representatives of Contractor, need access to DHS Protected Health Information in order for Contractor to perform the services described in the Contract:

- Kathy Holcomb_____
- Teri Lewis_____
- Brittany Greenway_____
- Mason Hall_____
- _____

Transfers of PHI must comply with DHS/DAS Policy and Procedures.

Approved methods of secure delivery of PHI between Contractor and AAA:

- Secure FTP file transfer (preferred)
- Encrypted email or email sent through "secure tunnel" approved by DHS Information Security Officer
- Email of encrypted document (password must be sent by telephone only)
- Encrypted portable media device and tracked delivery method

Contractor must update this list as needed and provide the updated form to DHS. Use of DHS Protected Health Information by individuals who are not described on this **Attachment A-1**, as amended from time to time, is impermissible and a violation of the Agreement. Contractor must update this **Attachment A-1** as needed and provide the updated form to DHS.

ATTACHMENT A-2

Part 1:
Please initial beside the correct option. Please select only one option.

_____ Contractor DOES NOT need any user accounts to access DHS Information Systems. Do not complete Part 2 of this form.

__kjh_____ Contractor DOES need user accounts to access DHS Information Systems. Please complete Part 2 of this form.

Part 2:
Please complete the table below if you indicated that Contractor DOES need any user accounts to access DHS Information Systems. Please attach additional pages if needed.

List of Individuals Authorized to Access a DHS Information System Containing PHI

The following individuals, as employees and/or representatives of Contractor, need access to DHS Information Systems containing DHS Protected Health Information in order for Contractor to perform the services described in the Contract:

Full Name	Employer	DHS Information System	Type of Access (Read only? Write?)
Teri Lewis	Habersham Senior Center	WellSky	Write
Brittany Greenway	Habersham Senior Center	Wellsky	Write
Mason Hall	Habersham Senior Center	Wellsky	Write
Kathy Holcomb	Habersham Senior Center	Wellsky	Write

Contractor must notify the AAA HCBS Manager and MIS Director identified in the Contract immediately, but at least within twenty-four (24) hours, after any individual on this list no longer needs the level of access described. Failure to provide this notification on time is a violation of the Agreement and will be reported as a security incident.

Contractor must update this **Attachment A-2** as needed and provide the updated form to AAA.