County of Fairfax, Virginia

AMENDMENT

Date: 7/28/2025

AMENDMENT NUMBER. 1

CONTRACT TITLE: Adolescent Detox and Crisis Residential

CONTRACTOR	SUPPLIER CODE	CONTRACT NUMBER
Northern VA BH, LLC, Northern, dba Virginia Adolescent Treatment Center 1600 Utica Avenue South, Suite 750 Minneapolis, MN 55416	1000058030	4400014143

By mutual agreement, Contract 4400013743 is amended as follows:

1. This Contract is hereby assigned to Northern VA BH, LLC, dba Northern Virginia Adolescent Treatment Center, renumbered and amended as summarized below:

	Original Information	New Information
Contractor Name	Acadia Healthcare	Northern VA BH, LLC, dba Northern Virginia Adolescent Treatment Center
Supplier ID	1000057383	1000058030
Contractor Address	6100 Tower Circle, Suite 1000 Franklin, TN 37067	6100 Tower Circle, Suite 1000 Franklin, TN 37067
Contact Information	Anthony Isom, Group CEO Anthony.isom@galaxrecovery.com	Anthony Isom, Group CEO Anthony.isom@galaxrecovery.com
Contract Number	4400013743	4400014143

2. Add the attached Business Associate/Qualified Service Organization (BAQSOA) Agreement and Breach Notification Risk Assessment Tool for Vendors (Appendix A) to the contract.

3. This amendment is effective immediately and in no way alters the prices, terms and conditions of the original contract. Northern VA BH, LLC, dba Northern Virginia Adolescent Treatment Center hereby assumes all responsibilities and obligations under the contract.

All other prices, terms, and conditions remain the same.

ACCEPTANCE:

BY: Anthony Isom
(Signature)

Group CEO
(Title)

Anthony Isom
(Printed)

7-22-2025
(Date)

DocuSigned by:
Lee Ann Pender
E239B762E600465...

Lee Ann Pender, CPPB
Director/County Purchasing Agent

DISTRIBUTION:
CSB: Wendy Rose
CSB: Sebastian Tezna
CSB: Rebecca Inch

Contractor: Anthony.isom@galaxyrecovery.com
DPMM Contract Specialist: Flor Morrobel

Department of Procurement and Material Management
12000 Government Center Parkway, Suite 427
Fairfax, VA 22035-0013
Website: www.fairfaxcounty.gov/procurement
Phone 703-324-3201, **TTY:** 711, **Fax:** 703-324-3228

FAIRFAX-FALLS CHURCH COMMUNITY SERVICES BOARD
BUSINESS ASSOCIATE/ QUALIFIED SERVICE ORGANIZATION AGREEMENT

This Business Associate/Qualified Service Organization Agreement ("Agreement") is entered into this 14th day of July 2025, by and between Fairfax County, doing business as the Fairfax-Falls Church Community Services Board ("CSB" or "Covered Entity"), and Northern VA BH, LLC, Northern, dba Virginia Adolescent Treatment Center ("Business Associate"), as defined in Section 1.1 below.

RECITALS

A. Fairfax County is a Hybrid Covered Entity. The County's covered components, including the CSB, are subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The CSB is also a "Part 2 Program," as defined by and the Confidentiality of Substance Use Disorder Patient Records, 42 C.F.R. Part 2, Subpart A through Subpart E, ("42 CFR Part 2"). The CSB provides services to residents of Fairfax County, the City of Falls Church, the City of Fairfax, the Town of Vienna, the Town of Herndon, the Town of Clifton, the George Mason University campus, and the Northern Virginia Community College campus.

B. Business Associate is a contractor providing Adolescent Detox and Crisis Residential Services in community-based sites for adolescents aged 13-17 for the Fairfax Falls Church Community Services Board.

C. The parties desire to enter into this Agreement regarding the use and/or disclosure of Protected Health Information ("PHI") as required by HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act (Division A, Title XIII and Division B, Title IV, of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5) (the "HITECH Act"), and their implementing regulations, including the Federal Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E (the "Privacy Rule"), the Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164, Subpart C (the "Security Rule"), and 42 CFR Part 2.

NOW, THEREFORE, in consideration of the mutual promises set forth herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. DEFINED TERMS.

1.1. Defined Terms. Capitalized terms used, but not otherwise defined in this Agreement, have the same meaning given to such terms in HIPAA, the HITECH Act, or the implementing regulations promulgated there under, including but not limited to the Privacy and Security Rules at 45 C.F.R. Part 160 and 45 C.F.R. Part 164. For purposes of this Agreement,

(a) "Covered Entity" means the CSB, and any Affiliate, and shall generally have the same meaning as the term "covered entity" at 45 C.F.R. § 160.103, and the term "Part 2 program" defined in 42 C.F.R. § 2.11;

(b) "Business Associate" means Northern VA BH, LLC, Northern, dba Virginia Adolescent Treatment Center in reference to this Agreement, and shall have the same meaning as the term "business associate" at 45 C.F.R. § 160.103, and the term "qualified service organization" as defined in 42 C.F.R. § 2.11;

(c) "Affiliate" means any entity that Controls, is under the Control of, or is under common Control with, the Covered Entity; "Affiliate" also means any entity that Controls, is under the Control of, or is under common Control with the Business Associate;

(d) "Control" or "Controls" means possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity;

FAIRFAX-FALLS CHURCH COMMUNITY SERVICES BOARD
BUSINESS ASSOCIATE/ QUALIFIED SERVICE ORGANIZATION AGREEMENT

(e) "Protected Health Information" or "PHI" means individually identifiable health information that is: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium. This term also refers to the Protected Health Information relating to Clients of the CSB and includes Patient Identifying Information as defined by 42 C.F.R. § 2.11.

(f) "Client" refers to patients and other individuals who receive and have received services from the Covered Entity, and for whom the Covered Entity maintains any PHI.

2. BUSINESS ASSOCIATE OBLIGATIONS.

2.1. Business Associate Status. Business Associate acknowledges and agrees that it is a "business associate" as defined by the Privacy and Security Rules.

2.2. Business Associate's Use or Disclosure of PHI. Business Associate may use or disclose PHI only as necessary to perform the services set forth in the parties' Contract 4400014143 and only to the extent such use or disclosure of PHI (a) would not violate the Privacy Rule if done by the CSB, (b) is reasonably limited to the minimum necessary information to accomplish the intended purposes of the use or disclosure; (c) is in compliance with each applicable requirement of 45 C.F.R. § 164.504(e); (d) is in compliance with the HITECH Act and its implementing regulations; and (e) is in compliance with 42 CFR Part 2. Business Associate shall not use or disclose PHI other than as permitted or required by this Agreement or by applicable law.

2.3. Safeguards for Protection of PHI.

(a) Business Associate will use appropriate safeguards to prevent use and/or disclosure of PHI other than as provided for by this Agreement.

(b) Business Associate will comply with applicable Security Rule provisions set forth at 45 C.F.R. Part 164, Subpart C, including provisions relating to Security Standards General Rules (45 C.F.R. §164.306), Administrative Safeguards (45 C.F.R. § 164.308), Physical Safeguards (45 C.F.R. § 164.310), Technical Safeguards (45 C.F.R. § 164.312), Organizational Requirements (45 C.F.R. §164.314) and Policies and Documentation (45 C.F.R. § 164.316), and implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic PHI that Business Associate creates, receives, maintains or transmits on behalf of the CSB.

(c) To the extent Business Associate is to carry out an obligation of the CSB under the Privacy Rule provisions set forth at 45 C.F.R. Part 164, Subpart E as directed by the CSB pursuant to the terms of this Agreement, Business Associate will comply with the requirements of the Privacy Rule that apply to the CSB in the performance of such obligation.

(d) To the extent Business Associate includes information received from the CSB in research reports, such information may only be published in aggregate form in which PHI has been rendered non-identifiable such that the information cannot be re-identified.

(e) To the extent Business Associate receives, stores, processes, or otherwise deals with substance use disorder patient records, it is fully bound by 42 CFR Part 2, including the requirement to resist any efforts to obtain access to PHI related to substance use disorder diagnosis, treatment, or referral for treatment except as permitted by 42 CFR Part 2. PHI protected by 42 CFR Part 2 may be disclosed only back to the CSB and may only be used as authorized by this Agreement or 42 CFR Part 2.

(f) Business Associate will retain records in compliance with applicable record retention laws and will comply with applicable record security provisions of 42 C.F.R. § 2.16 for the maintenance and destruction of PHI contained in substance use disorder patient records.

2.4. Notification.

(a) Business Associate will promptly report to Fairfax County's HIPAA Compliance Officer any use or disclosure of PHI not provided for by this Agreement of which Business Associate becomes aware. This includes, but is not limited to, reporting breaches of Unsecured Protected Health Information as required at 45 C.F.R. 164.410.

(b) Business Associate will report to Fairfax County's HIPAA Compliance Officer any Security Incident of which it becomes aware, in the following time and manner:

i. any actual, successful Security Incident will be reported in writing within three (3) business days of the Business Associate's discovery of such actual, successful Security Incident.

ii. For any actual, successful Security Incident, or for any attempted, unsuccessful, Security Incident of which Business Associate becomes aware, Business Associate shall promptly complete a breach assessment tool (Appendix A) and provide the completed assessment to Fairfax County's HIPAA Compliance Officer within three (3) business days of completion.

(c) Subject to any law enforcement delay required under 45 C.F.R. § 164.412, Business Associate will report to Fairfax County's HIPAA Compliance Officer in writing any Breach of Unsecured PHI within three (3) business days of discovery, and any such report shall include the identification of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used or disclosed as a result of any such potential Breach, together with such other information regarding the potential Breach as is known to Business Associate at the time such report is made (such as the type of PHI involved in the event, the nature of the information accessed, acquired or disclosed, etc.) or promptly thereafter as such other information becomes available.

i. The CSB may require Business Associate to provide Notice to Individuals affected by a Breach caused by Business Associate, as required by 45 C.F.R. § 164.404. If the CSB provides the required Notice to Individuals as a result of Business Associate's Breach, the CSB reserves the right to be reimbursed by Business Associate all direct and indirect costs related to providing such Notice.

2.5. Mitigation. Business Associate will mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement or as the result of any Security Incident known to Business Associate.

FAIRFAX-FALLS CHURCH COMMUNITY SERVICES BOARD
BUSINESS ASSOCIATE/ QUALIFIED SERVICE ORGANIZATION AGREEMENT

2.6. Cooperation. Business Associate will work cooperatively with the CSB in connection with the CSB's investigation of any Breach and in connection with any notices the CSB determines are required as a result.

2.7. Subcontractors. Business Associate will ensure that any subcontractor that creates, receives, maintains or transmits PHI on behalf of Business Associate agrees to the same restrictions and conditions that apply through the applicable Engagement and this Agreement to Business Associate with respect to such PHI.

2.8. Client Rights Regarding PHI. The Privacy Rule grants Clients certain rights with regard to the PHI maintained in a "Designated Record Set" (as such term is defined in 45 C.F.R. § 164.501) about them. The CSB hereby agrees that the PHI provided to Business Associate shall not constitute a Designated Record Set or shall be limited to duplicates of information maintained in a Designated Record Set by the CSB. However, to the extent Business Associate maintains PHI for an Individual in a Designated Record Set, Business Associate shall provide access to such PHI to the CSB or, as directed by the CSB, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524. Business Associate shall document disclosures of PHI and such information related to such disclosures as would be required for the CSB to respond to a request by a Client for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 (and HITECH Act § 13405(c) when such requirements are effective as to the CSB), and shall provide such information to the CSB promptly upon written request by the CSB. Business Associate shall notify the CSB promptly if Business Associate receives a request from a Client to access, amend or receive an accounting of disclosures of Client's PHI.

2.9. Books and Records.

(a) If Business Associate receives a request from the Secretary of Health and Human Services (the "Secretary") that Business Associate make available its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, the CSB, to the Secretary for purposes of determining The CSB's compliance with the Privacy Rule, Business Associate shall promptly notify the CSB that it has received such a request. Upon Business Associate's receipt of a written directive to do so from the CSB, Business Associate will make the relevant internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary.

(b) Nothing in this section shall be construed to require Business Associate to disclose or produce to the Secretary communications that are subject to attorney-client privilege held by Business Associate with respect to legal advice it seeks from other legal counsel. Although Business Associate and the CSB are making a good faith effort to achieve conformance of these terms and conditions with the requirements of applicable law, the CSB acknowledges that Business Associate has not represented or warranted to the CSB, that these terms and conditions, including the procedures outlined in this paragraph, will be deemed by the Secretary or a court to satisfy the requirements of the Privacy and Security Rules or the HITECH Act.

(c) Fairfax County's HIPAA Compliance Officer may make a written request that Business Associate make available its internal HIPAA documents and records, whether in hardcopy or electronic form, to the County for purposes of determining Business Associate's compliance with HIPAA. For purposes of this BAA, "internal HIPAA documents and records" means HIPAA policies and procedures, risk assessments, training records, electronic systems, and other practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Fairfax County. Upon Business Associate's receipt of the written request, Business Associate will make the relevant internal records available to Fairfax County's HIPAA Compliance Officer.

2.10. Use or Disclosure for Business Associate Administration.

Except as otherwise limited by the terms of this Agreement:

(a) Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate; and

(b) Business Associate may disclose PHI for the proper management and administration of Business Associate, provided that disclosures are Required by Law or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

2.11. Reporting of Violations of Law. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with the Privacy Rule.

3. OBLIGATIONS OF COVERED ENTITY.

3.1. Notice of Privacy Practices. As applicable, the CSB shall notify Business Associate in writing of any and all limitations in its notice of privacy practices or its policies or procedures to the extent that any such limitation may affect Business Associate's use or disclosure of PHI.

3.2. Notice of Modifications. The CSB shall notify Business Associate in writing of any changes in, or revocation of, an authorization or other permission by a Client to use or disclose PHI to the extent that such change or revocation may affect the use or disclosure of PHI by Business Associate or its subcontractors.

3.3. Special Restrictions. The CSB shall notify Business Associate in writing of any restriction to the use or disclosure of PHI that the CSB has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

3.4. Scope of Requests for Use or Disclosure. Except for the uses and disclosures of PHI contemplated by Sections 2.2 and 2.10 above, the CSB shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA, the HITECH Act, their implementing regulations, or 42 CFR Part 2, if done by the CSB.

FAIRFAX-FALLS CHURCH COMMUNITY SERVICES BOARD
BUSINESS ASSOCIATE/ QUALIFIED SERVICE ORGANIZATION AGREEMENT

4. TERM AND TERMINATION.

4.1. Term. This Agreement shall be effective on the date first written above and shall expire upon termination of the parties' underlying Contract.

4.2. Termination by Covered Entity. Upon the CSB's becoming aware of a breach of this Agreement by Business Associate, the CSB shall provide written notice of and an opportunity for Business Associate to cure the breach or end the violation of the Agreement. If the breach is not cured or the violation is not terminated within forty-five (45) days of the date of such notice the CSB may terminate this Agreement. Multiple breaches of this Agreement or violations by the Business Associate may result in termination of this Agreement with thirty (30) days' notice to Business Associate and without an opportunity to cure any further breach or violation.

4.3. Return of PHI. Upon any termination, expiration or non-renewal of this Agreement, Business Associate will return or, at the request and expense of the CSB, destroy any PHI that Business Associate, its agents, or subcontractors then maintains in any form. If, however, Business Associate or the CSB determine that such return or destruction is not feasible, such PHI will not be returned or destroyed and Business Associate will remain bound by the provisions of this Agreement as to such retained PHI until such PHI is returned to the CSB or destroyed.

5. MISCELLANEOUS

5.1. Notices. Any notice required or permitted under this Agreement will be given in writing to:

the Covered Entity at:

Tanya Bullock, HIPAA Compliance Officer
12000 Government Center Parkway, Suite 553
Fairfax, VA 22035
Phone: (703) 324-2164

to the Business Associate at:

6100 Tower Circle, Suite 1000
Franklin, TN 37067

Notices will be deemed to have been received upon actual receipt, one business day after being sent by overnight courier service, or five (5) business days after mailing by certified or priority mail, whichever occurs first.

5.2. Governing Law. This Agreement will be governed by, and construed in accordance with, the laws of the Commonwealth of Virginia, without regard to its conflicts of laws principles.

5.3. No Third-Party Beneficiaries. This Agreement shall not in any manner whatsoever confer any rights upon or increase the rights of any third party.

5.4. Waiver. No delay or omission by either party to exercise any right or remedy under this Agreement will be construed to be either acquiescence or the waiver of the ability to exercise any right or remedy in the future.

5.5. Severability. In the event any part or parts of this Agreement are held to be unenforceable, the remainder of this Agreement will continue in effect.

FAIRFAX-FALLS CHURCH COMMUNITY SERVICES BOARD
BUSINESS ASSOCIATE/ QUALIFIED SERVICE ORGANIZATION AGREEMENT

5.6. Amendments. This Agreement may not be modified in any respect other than by a written instrument signed by both parties.

5.7. Assignment. This Agreement is not assignable by either party without the other party's written consent.

5.8. Renegotiation. The parties agree to negotiate in good faith any modification to this Agreement that may be necessary or required to ensure consistency with amendments to and changes in applicable federal and state laws and regulations, including but not limited to, HIPAA, the Privacy and Security Rules, the HITECH Act, regulations promulgated pursuant to HIPAA or the HITECH Act, and 42 CFR Part 2.

5.9. Regulatory and Statutory References. Any reference in this Agreement to HIPAA, the HITECH Act, the Privacy Rule the Security Rule, other regulations implementing HIPAA or the HITECH Act, or 42 CFR Part 2 shall mean such statute or regulation as in effect at the time of execution of this Agreement or, if and to the extent applicable, as subsequently updated, amended or revised.

5.10. Interpretation. Any ambiguity in the Agreement shall be resolved in favor of a meaning that permits the parties to comply with HIPAA and 42 CFR Part 2.

5.11. Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

5.12. Scope and Effect of Agreement. This Agreement sets forth the entire agreement and understanding between the parties relating to the subject matter hereof and supersedes and replaces, from the date of this agreement, all other prior discussions, representations, agreements and understandings of every kind or nature, whether oral or written, with respect to the subject matter here of, including without limitation each previously existing business associate agreement, if any, between Business Associate and the Covered Entity.

5.13. Survival. The provisions of Section 4.3 and Section 5 shall survive the termination of this Agreement.

IN WITNESS THEREOF, the parties have executed this Agreement as of the dates written below.

Northern VA BH, LLC	**Fairfax County Government**
(Business Associate)	(Covered Entity)
By: Anthony Ison	By: DocuSigned by: Lee Ann Pender E230B762E600465...
Name and Title: Anthony Ison, Group CEO	Name and Title: Lee Ann Pender Director
Date: 7-22-2025	Date: 7/28/2025

HIPAA Compliance Program

Breach Notification Risk Assessment Tool

Summary of HIPAA Breach Notification Rule, 45 CFR § 164.400-414

The Fairfax County HIPAA Compliance Program and the HIPAA Breach Notification Rule requires HIPAA covered entities[functions] and their business associates to provide notification following a breach of unsecured protected health information (PHI). A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of protected health information. An impermissible use or disclosure is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates through a thorough risk assessment (as outlined below) that there is a low probability that the PHI has been *compromised* based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used or had access to the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Was Protected Health Information (PHI) Involved? PHI is health information that identifies, or there is a reasonable basis to believe it can be used to identify, the individual. Health information includes any demographic information of the individual (e.g. name, address, birth date, Social Security number, medical record number) and information relating to the physical or mental health or condition of an individual, the health care provided to an individual (e.g. diagnosis, treatment plan, medication, medical history and test results), or payment for health care provided to an individual:

☐ Yes ☐ No

If yes, PHI was involved, please continue completing this risk assessment tool.
If no, PHI was not involved, then no breach occurred.

Date Incident Occurred:

Date Incident Reported:

Breach Notification Due Date:
(If applicable, 60 days from incident report date)

HIPAA Compliance Program

Breach Notification Risk Assessment Tool

Name & Title of Person Who Reported Incident:

Brief Description of Incident

1. Who accessed or disclosed the PHI?
2. Was the person authorized to access the PHI? Explain why or why not.
3. How did the person access and/or disclose the PHI? Explain in detail.
4. What was the person's explanation for accessing and/or disclosing the PHI?
5. Was the PHI received by the intended recipient?
6. What did the intended recipient do with the PHI? Was the PHI forwarded to any other person or entity?
7. Was the PHI recovered and/or did the HIPAA Privacy & Security Officers receive confirmation that the PHI was destroyed?
8. Was the incident reported to law enforcement? If so, include name of agency, name of contact at agency (if known), date reported, report number and known status.

Description of PHI (*e.g., Type of Information, Fields, # of Records*):

HIPAA Compliance Program

Breach Notification Risk Assessment Tool

Was PHI accessed, used, or disclosed as permitted by the Privacy Rule? (Was use or disclosure limited to the "minimum necessary" for treatment, payment and health care operations (TPO)?)

☐ Yes ☐ No

If yes, PHI was accessed, used or disclosed as permitted by the Privacy Rule, then no breach occurred and you may conclude this assessment. Reporting is not required under HIPAA.

If no, PHI accessed, used or disclosed was not limited to the "minimum necessary" for TPO, please continue to the next question.

Was information held by <insert name of organization> in its capacity as an employer? (For example, <name of organization> obtains PHI from another entity and uses/discloses PHI information for purposes of FMLA, Workers Compensation, and/or HR employment related activities. If <name of organization>obtains and uses PHI in this capacity, then it is not considered PHI and not considered a breach.)

☐ Yes ☐ No

If yes, then no breach occurred and you may conclude this assessment. Reporting is not required under HIPAA.

If no, then please continue to the next question.

Was PHI encrypted, destroyed or properly de-identified (limited data set with no direct identifiers *and* does not include dates of birth or zip codes)?

☐ Yes ☐ No

If yes, then no breach occurred and you may conclude this assessment. Reporting is not required under HIPAA.

If no, then please continue to the next question.

HIPAA Compliance Program

Breach Notification Risk Assessment Tool

Does an exception to the Breach Notification Rule apply? Please review Exceptions A-C below.

☐ Yes ☐ No

If yes, Exception A, B or C applies (please check one below), then no breach occurred and you may conclude this assessment. Reporting is not required under HIPAA.

If no, Exception A, B or C does not apply, then please continue to the Risk Assessment below.

☐ **Exception A.** Was PHI unintentionally accessed or used by a workforce member (employee, volunteer, trainee) or person acting under the authority of a covered entity or business associate within his/her scope of authority, and the PHI was not further impermissibly used/disclosed?

☐ Yes ☐ No

Briefly explain your answer:_____

_____

☐ **Exception B.** Was PHI inadvertently disclosed by an authorized person at a covered entity or business associate to another authorized person at the same covered entity or business associate, and the PHI was not further impermissibly used/disclosed?

☐ Yes ☐ No

Briefly explain your answer:_____

_____

☐ **Exception C.** Does covered entity or business associate have a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information? (For example, PHI sent via mail to the wrong address and returned unopened could not reasonably have been read or retained by the improper addressees.)

☐ Yes ☐ No

Briefly explain your answer:_____

_____

Risk Assessment

An acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a breach and must be reported unless the covered entity demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors listed below.

Can this breach be determined to have a ***low probability*** that the PHI was compromised based on the following assessment?

HIPAA Compliance Program

Breach Notification Risk Assessment Tool

1) What type and amount of PHI was involved and how likely is it that individuals could be identified if PHI is combined with other available information? Consider whether more sensitive identifiable information was involved (e.g., date of birth, SSN, financial information) or sensitive clinical information (e.g. mental health, test results, STD results) that could increase the risk of identity theft, financial fraud, reputational or other harm to the individual.

☐ Yes, this factor supports low probability of compromise. ☐ No

Describe the nature and amount of the PHI:

2) Who impermissibly used the PHI and/or to whom was the PHI impermissibly disclosed? Consider this factor if the PHI was impermissibly used or disclosed within or outside of the County. Consider whether the person has legal obligations to protect the information. For example, is the person a covered entity required to comply with HIPAA, or a government employee, etc.? If so, there may be a lower probability that the PHI has been compromised.

☐ Yes, this factor supports low probability of compromise. ☐ No

Describe who received or used the PHI:

3) Was the PHI actually acquired or viewed or was there only the opportunity to acquire or view but actual viewing or acquisition of PHI did not occur? (If electronic PHI is involved, this may require a forensic analysis of the computer to determine whether the PHI was accessed, viewed, acquired, transferred or otherwise compromised.)

☐ Yes, this factor supports low probability of compromise. ☐ No

Describe whether the PHI was actually acquired or viewed:

4) To what extent was the risk to the PHI mitigated? For example, by obtaining the recipient's satisfactory assurances that the PHI will not be further used or disclosed (through a confidentiality agreement, declaration or similar means), has been returned, or has been/will be destroyed.

☐ Yes, this factor supports low probability of compromise. ☐ No

Describe steps <name of organization>took or intends to take to mitigate risk:

HIPAA Compliance Program

Breach Notification Risk Assessment Tool

Breach Risk Assessment Result

<Name of organization> performed a breach risk assessment, as required under the Department of Health and Human Services, Breach Notification for Unsecured Protected Health Information; Final Rule, effective on March 26, 2013 and reached the following conclusion.

☐ **Breach notification is required.** <Name of organization> concludes that notification is required because the assessment above supports that there is greater than low probability that the PHI has been compromised.

☐ **Breach notification is not required. <Name of organization>** concludes that notification is not required because the assessment above supports that there is a low probability that the PHI has been compromised.

Scope of Notification ***(Note: If more than 500 individuals OCR and Media Notice is required)***

Other corrective action(s) required:

- DIT corrective actions(s)

- Manager(s) responsible for implementing corrective action:

Date corrective action should be delivered:

- Date of corrective action; confirmation by the HIPAA Compliance Officer

HIPAA Compliance Officer Analysis:

HIPAA Compliance Program

Breach Notification Risk Assessment Tool

Preventive action(s) required:
Describe who, what, when and how the preventative action(s) will be carried out:

HIPAA/HITECH Decision Tree to Determine Whether Breach Notification is Required