SEPA Labs	Policy & Procedure HIPAA / PRIVACY **BUSINESS ASSOCIATES**	FUNCTION
		NUMBER 4a
		PRIOR ISSUE
		EFFECTIVE DATE January 1, 2014

PURPOSE

The purpose of this Policy is to provide a process for establishing a written agreement with each of SEPA Labs's Business Associates ("BA") as required by the HIPAA Privacy Rule.

POLICY

SEPA Labs contracts with various outside entities and organizations to perform functions or provide services on behalf of SEPA Labs that may involve the disclosure of Protected Health Information ("PHI") to the outside entity. These outside entities are SEPA Labs's Business Associates. The policy of this Facility is to obtain written assurances from BAs that they will appropriately safeguard any PHI they create or receive on SEPA Labs's behalf. Such written assurances will be in place before SEPA Labs discloses PHI to the Business Associate.

PROCEDURE

1. SEPA Labs Administrator will follow established procedures regarding contract review, revision and approval to assure that contract is in compliance with state and federal law.
2. For each contract, determine whether a Business Associate Agreement is necessary. (See the "Business Associate Decision Tree" following this Policy.) Common examples of BAs are:
   a. SEPA Labs's Billing Service
   b. An attorney who reviews patient information to assist in laboratory services or problems
   c. Laboratory Outside Accountants or Consultants

   Note: Business Associate language is ***not*** required when the BA is a health care provider and all disclosures to the BA concern the treatment of a patient.
3. If a BA Agreement is necessary and the third party provides its own BA Agreement, review the Agreement to assure it meets all requirements of the Privacy Rule. (See "Business Associate Checklist" following this Policy.)
4. If a BA Agreement is necessary, and the third party does not provide the Agreement, submit Facility's template BA Agreement for approval by the third party.
5. If the BA refuses to sign the BA Agreement, the HIPAA Privacy Rule prohibits SEPA Labs from disclosing any PHI to the BA. If the BA requires access to PHI in order to perform the function or service on behalf of SEPA Labs, SEPA Labs shall not contract with the BA.
6. The original signed contract and contract addendum containing BA language shall be maintained by SEPA Labs.

7. Violations of BA Requirements - If SEPA Labs staff learns of a breach or violation of a BA requirement by a BA, such breach or violation shall be reported to the Privacy Officer, his designee, or to the Compliance Department. The Privacy Officer or Compliance Designee will assist SEPA Labs in determining whether reasonable steps can be taken to cure the breach. If SEPA Labs's reasonable steps to cure the BA's violations are unsuccessful, SEPA Labs may:

   a. Terminate the contract or arrangement; or

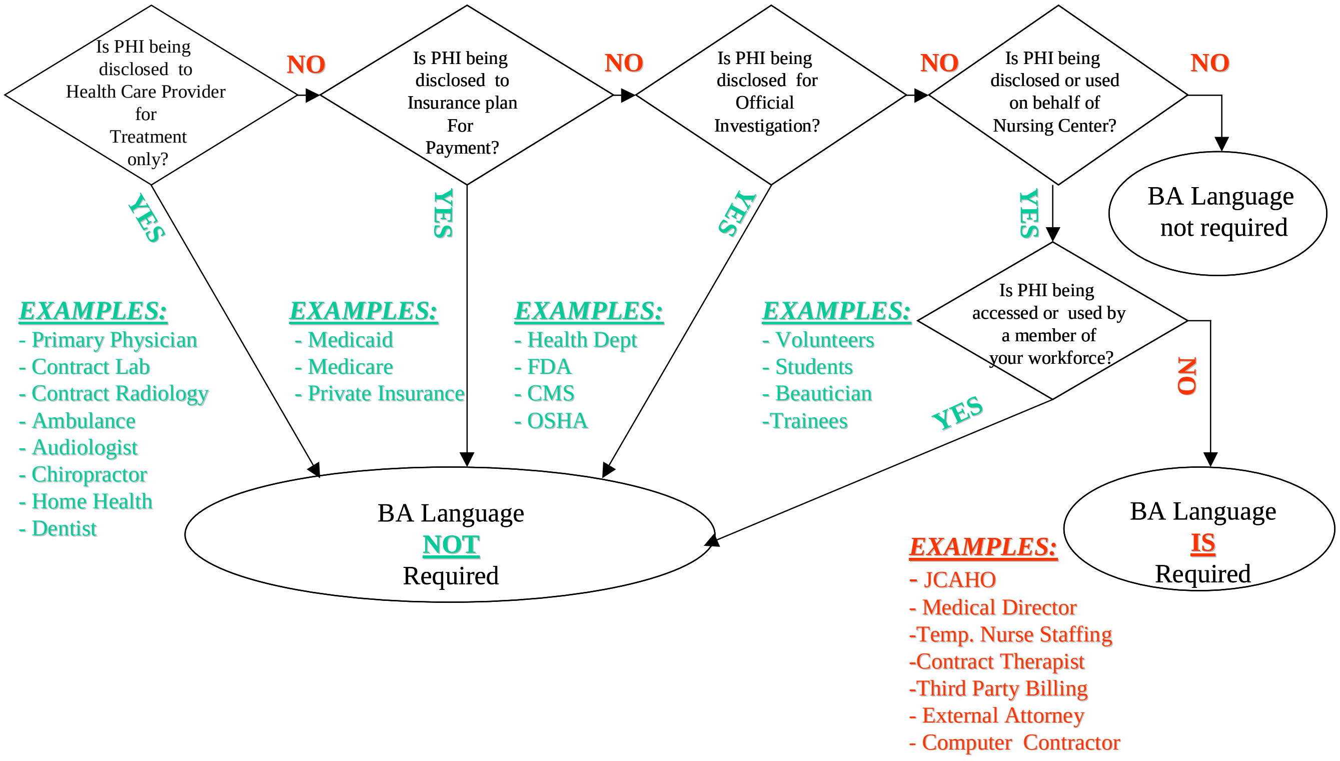
   b. If termination is not feasible, report the problem to the Secretary of the U. S. Department of Health and Human Services.

8. Notice of Termination of a Contract with a BA - SEPA Labs shall notify the Privacy Officer, his designee or the Legal Department when issuing or receiving a notice of contract termination involving a BA. The Legal Department will assist with contacting the BA regarding the BA's obligations to return or destroy all PHI or, if return or destruction is not feasible, to extend the protections of the BA requirements to the PHI and to limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

   The contract and contract addendum must be retained for six years after the contract was last in effect.

SEPA Labs	**Policy & Procedure** HIPAA / PRIVACY **BUSINESS ASSOCIATES**	**FUNCTION**
		NUMBER 4a
		PRIOR ISSUE
		EFFECTIVE DATE January 1, 2014

DECISION TREE: WHEN IS BA LANGUAGE REQUIRED?



SEPA Labs	**Policy & Procedure**	**FUNCTION**
	HIPAA / PRIVACY **BUSINESS ASSOCIATES**	**NUMBER** 4a
		PRIOR ISSUE
		EFFECTIVE DATE January 1, 2014

This page intentionally left blank.

SAMPLE
BUSINESS ASSOCIATE CHECKLIST

Contract Provision	***Reg. Cite***	***Requirement***	***Related provisions, comments***
	164.504(e)(2)(i)	Establish permitted and required uses and disclosures of PHI by BA	Final rule – must generally state purposes, reasons for use/disclosure and types of persons to whom info can be disclosed
	164.504(e)(2)(i)	May not authorize BA to use or further disclose info in a manner that would violate requirements of subpart if done by CE **except:** ↓	Must include "minimum necessary" language, either within this clause, or as a separate clause. *BA shall use/disclose PHI only in the minimum amount and to the minimum number of individuals necessary to achieve the purpose of the services being rendered to or on behalf of CE.*
	164.504(e)(2)(i)(A)	May permit BA to use or disclose PHI for "proper management & administration of BA as permitted by **(e)(4)**	
	164.504(e)(4)(i)(A) and (B)	May permit BA to **use** PHI – in its capacity as a BA if necessary for the proper management & administration of BA **or** to carry out the legal responsibilities of BA.	
	164.504(e)(4)(ii)	May permit BA to **disclose** PHI – in its capacity as a BA for same purposes, **but only if disclosure is** →	
	164.504(e)(4)(ii)(A)	Required by law **or** ↓	
	164.504(e)(4)(ii)(B)(1)	BA obtains reasonable assurances from person to whom info is disclosed that info will be held confidentially and used or further disclosed only as required by law or for purpose for which it was disclosed to the person **AND** →	
	164.504(e)(4)(ii)(B)(2)	The person to whom the information was disclosed notifies BA of any instance of which it is aware in which the confidentiality of the information has been breached.	
	164.504(e)(2)(i)(B)	BA may provide data aggregation services relating to the health care operations of the covered entity.	

Contract Provision	***Reg. Cite***	***Requirement***	***Related provisions, comments***
	164.504(e)(2)(ii)(A)	BA will not use or further disclose the information other than as permitted or required by the contract or as required by law.	
	164.504(e)(2)(ii)(B)	BA will use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract.	
	164.504(e)(2)(ii)(C)	BA will report to the CE any use or disclosure of the information not provided for by its contract of which it becomes aware.	Negotiate time and manner of reporting with BA – in writing, to whom, time frame, etc.
	164.504(e)(2)(ii)D	BA will ensure that any agents, including a subcontractor, to whom it provides PHI received from, or created or received by the BA on behalf of, the CE agrees to the same restrictions and conditions that apply to the BA with respect to such information.	May want BA to list subcontractors and agents in exhibit.
	164.504(e)(2)(ii)E	<u>Access</u>: BA will make available PHI in accordance with **164.524.**	Not necessary if BA does not have PHI in a designated record set.
	164.504(e)(2)(ii)F	<u>Amendment</u>: BA will make available PHI for amendment and incorporate any amendments to PHI in accordance with **164.526.**	Not necessary if BA does not have PHI in a designated record set.
	164.504(e)(2)(ii)G	<u>Accounting</u>: BA will document disclosures of PHI as would be required for CE to respond to a request for an accounting.	
	164.504(e)(2)(ii)G	<u>Accounting</u>: BA will make available PHI to provide an accounting of disclosures in accordance with **164.528.**	
	164.504(e)(2)(ii)H	BA will make internal practices, etc. available to the Secretary.	
	164.504(e)(2)(ii)I	<u>Termination</u>: BA will – if feasible – return or destroy all PHI received from, or created or received by the BA on behalf of the CE. BA will retain no copies of such information. If return or destruction of such information is not feasible, BA will extend the protections of the K to the information and limit further uses and disclosures to those purposes that make the return or the destruction of the information infeasible.	
	164.504(e)(2)(iii)	Authorize termination by CE if CE determines that the BA has violated a material term of the contract.	
	Not required by Privacy Rule	<u>MITIGATION</u>	Not required by law, but included in sample language in August final rule.

Contract Provision	***Reg. Cite***	***Requirement***	***Related provisions, comments***
	Not required by Privacy Rule	INSURANCE	If main contract has insurance clause, may not be necessary in addendum.
	Not required by Privacy Rule	Inspection Allow CE to inspect BA’s systems, books, records if CE becomes aware of a breach	CE is not required to monitor BA’s activities for Privacy Rule purposes.
	Not required by Privacy Rule	INDEMNIFICATION	If main contract has indemnification clause, may not be necessary in addendum.
	Not required by Privacy Rule	Interpretation/ambiguity – broadly as necessary to implement and comply with the Privacy Rule and applicable state laws. Any ambiguity shall be resolved in favor of a meaning that complies and is consistent with the Privacy Rule.	
	Not required by Privacy Rule	Amendment to comply with law - Modification of K to be in compliance with Privacy Rule	
	Not required by Privacy Rule	Assistance in litigation or administrative proceedings	If main contract has this type of clause, may not be necessary in addendum.
	Not required by Privacy Rule	Conflict with contract – addendum controls as it relates to PHI	

This page intentionally left blank.