HIPAA Notice of Privacy Practices

Effective 9/1/2020
Reviewed: 9/17/2021, 8/23/2022, 9/13/2023, 8/7/2024, 7/31/2025, 5/5/2026

Joint Venture Hospital Laboratories (JVHL)
999 Republic Dr., Suite 300
(800) 445-4979

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT A PATIENT MAY BE USED AND DISCLOSED AND HOW A PATIENT CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This Notice of Privacy Practices describes how JVHL may use and disclose a patient's protected health information (PHI) to carry out treatment, payment or health care operations (TPO) and for other purposes that are permitted or required by law. It also describes the patient's rights to access and control their protected health information. "Protected health information" is information about a patient, including demographic information, that may identify the patient and that relates to a patient's past, present or future physical or mental health condition and related health care services.

Recent Updates to the HIPAA Privacy Rule
In response to recent changes in law and regulation, including updates to support reproductive health and to address proposals made in the Notice of Proposed Rulemaking for the Confidentiality of Substance Use Disorder (SUD) Patient Records ("Part 2 NPRM"), as required by or consistent with the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020, we have updated our privacy practices as follows:

USES AND DISCLOSURES OF PROTECTED HEALH INFORMATION (PHI)

Protected health information may be used and disclosed by JVHL, our office staff and others outside of our office that are involved in a patient's care and treatment for the purpose of providing health care services to a you, to pay your health care bills, to support the operations of JVHL, and any other use required by law.

Treatment: We will use and disclose your protected health information to provide, coordinate, or manage your health care and any related services. This includes the coordination or management of your health care with a third party. For example, your protected health information may be provided to your health plan to ensure appropriate oversight of your treatment plan.

Payment: Your protected health information will be used, as needed, to obtain payment for your health care services. For example, obtaining additional medical records to support payment for a procedure.

Healthcare Operations: We may use or disclose, as-needed, your protected health information in order to support the business activities of your physician's practice. These activities include, but are not limited to, providing lab results as requested by your physician to disease management systems that are utilized to align with required performance criteria for your care.

Specific Uses and Disclosures

Reproductive Health Information: In accordance with the updated HIPAA Privacy Rule, we are committed to ensuring the confidentiality and security of your reproductive health information. This includes any information related to family planning, pregnancy, contraception, fertility treatments, and other related services. We will not disclose this information without your explicit authorization, except as required by law or in specific circumstances such as:

- To Your Healthcare Providers: For treatment purposes to ensure continuity of care.
- To Public Health Authorities: If required by law for public health reporting.
- To Prevent Serious Threats: If necessary to prevent a serious threat to health or safety.

Substance Use Disorder Records: In compliance with the CARES Act and the 2024 Part 2 Final Rule we will maintain the confidentiality of your substance use disorder treatment records and only disclose them with your consent, except as required or permitted by law.

We may use or disclose your protected health information in the following situations without your authorization. These situations include: as required by law, public health issues as required by law, communicable diseases, health oversight, abuse or neglect, food and drug administration requirements, legal proceedings, law enforcement, coroners, funeral directors, organ donation, research, criminal activity, military activity and national security, workers' compensation, inmates, and other required uses and disclosures. Under the law, we must make disclosures to you upon your request. Under the law, we must also disclose your protected health information when required by the Secretary of the Department of Health and Human Services to investigate or determine our compliance with the requirements under Section 164.500.

Other Permitted and Required Uses and Disclosures will be made only with your consent, **authorization** or opportunity to object unless required by law. **You may revoke the authorization**, at any time, in writing, except to the extent that your physician or the physician's practice has taken an action in reliance on the use or disclosure indicated in the authorization.

YOUR RIGHTS

The following are statements of your rights with respect to your protected health information.

You have the right to inspect and copy your protected health information (fees may apply) – Under federal law, however, you may not inspect or copy the following records: Psychotherapy notes, information compiled in reasonable anticipation of, or used in, a civil, criminal, or administrative action or proceeding, protected health information restricted by law, information that is related to medical research in which you have agreed to participate, information whose disclosure may result in harm or injury to you or to another person, or information that was obtained under a promise of confidentiality.

JVHL will charge a fee for the copy of the patient's PHI or for a summary of the PHI, as allowed under applicable law:

1. Flat fee for electronic copies of PHI maintained electronically = $6.50
2. Fees for paper copies of PHI*:*
   Search Fee = $25.38
   Pages 1 – 20 = $1.27 per page
   Pages 21 – 50 = $0.63 per page
   Pages 51+ = $0.25 per page

You have the right to request a restriction of your protected health information – This means you may ask us not to use or disclose any part of your protected health information for the purposes of treatment, payment or healthcare operations. You may also request that any part of your protected health information not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice of Privacy Practices. Your request must state the specific restriction requested and to whom you want the restriction to apply. Your physician is not required to agree to your requested restriction.

You have the right to request to receive confidential communications – You have the right to request confidential communication from us by alternative means or at an alternative location. You have the right to obtain a paper copy of this notice from us, upon request, even if you have agreed to accept this notice alternatively i.e. electronically.

You have the right to request an amendment to your protected health information – If we deny your request for amendment, you have the right to file a statement of disagreement with us and we may prepare a rebuttal to your statement and will provide you with a copy of any such rebuttal.

You have the right to receive an accounting of certain disclosures – You have the right to receive an accounting of all disclosures except for disclosures: pursuant to an authorization, for purposes of treatment, payment, healthcare operations; required by law, that occurred prior to April 14, 2003, or six years prior to the date of this request.

You have the right to obtain a paper copy of this notice from us even if you have agreed to receive the notice electronically. We reserve the right to change the terms of this notice and we will notify you of such changes. We will also make available copies of our new notice if you wish to obtain one.

COMPLAINTS

You may complain to us or to the Secretary of Health and Human Services if you believe your privacy rights have been violated by us. You may file a complaint with us by notifying our Privacy Officer of your complaint. Our Privacy Officer can be reached via email at privacy@jvhl.org. **We will not retaliate against you for filing a complaint.**

We are required by law to maintain the privacy of, and provide individuals with, this notice of our legal duties and privacy practices with respect to protected health information. We are also required to abide by the terms of the notice currently in effect. If you have any questions in reference to this form, please ask to speak with our HIPAA Compliance Officer in person or by phone at our main phone number, (800) 445-4979.

Please sign the accompanying "Acknowledgment" form. Please note that by signing the Acknowledgment form you are only acknowledging that you have received or been given the opportunity to receive a copy of our Notice of Privacy Practices

Strictly Necessary Cookies Active

Always Active: These cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as acknowledging our cookie consent, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site will not then work. These cookies do not store any personally identifiable information.

Acknowledgment of Our Notice of Privacy Practices

I hereby acknowledge that I have received or have been given the opportunity to receive a copy of JVHL's Notice of Privacy Practices. By signing below, I am "only" giving acknowledgment that I have received or have had the opportunity to receive the Notice of our Privacy Practices.

_____

Patient Name (Type or Print) Date

_____

Signature

Strictly Necessary Cookies Active

Always Active: These cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as acknowledging our cookie consent, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site will not then work. These cookies do not store any personally identifiable information.

Sample Business Associate Agreement

JVHL BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") is made and entered into between **Joint Venture Hospital Laboratories, LLC("JVHL")** (or "Company"), having its principal place of business at **999 Republic Drive, Suite 300, Allen Park, MI 48101** and _____ ("Business Associate or "BA"), having its principal place of business at _____.

RECITALS:

Company is a "covered entity" within the meaning of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), the standards for the privacy of Individually Identifiable Health Information (the "Privacy Rule") and the standards for the security of Electronic Protected Health Information (the "Security Rule") promulgated by the United States Department of Health and Human Services ("DHHS") pursuant thereto.

BA provides _____ service to Company, which services necessarily involve the access to, generation of, use of, or disclosure of health information that identifies individual patients (protected health information or "PHI"), some of which is in electronic form ("Electronic Protected Health Information" or "EPHI"). Accordingly, _____ is a business associate of Company pursuant to HIPAA, the HITECH Act, the Privacy Rule and the Security Rule.

Company is obligated by HIPAA, the Privacy Rule and the Security Rule to obtain "satisfactory assurances" from its business associates as a precondition to permitting a business associate to access, generate, use, or disclose PHI and EPHI on its behalf or in the course of performing services for it.

For the foregoing reasons, Company and BA desire to enter into an agreement that complies with all the requirements of HIPAA, the HITECH Act, the Privacy Rule and Security Rule regarding business associate "satisfactory assurances."

NOW THEREFORE, in consideration of the foregoing and of the mutual promises contained herein, Company and BA agree as follows:

Obligations of Business Associate

Pursuant to the Privacy Rule and Security Rule, BA shall:

1. Not use or further disclose protected health information, as defined by the Privacy Rule, and specifically including electronic protected health information defined by the Privacy Rule ("Electronic Protected Health Information," collectively "PHI"), other than

    a. For the proper management and administration of JVHL;

    b. To carry out the legal and/or contractual responsibilities of JVHL, including its responsibilities under its provider participation agreement with Company and the contracts with health plans that are entered into pursuant to the transactions contemplated by the provider participation agreement;

    c. To provide data aggregation services relating to the health care operations of the Company pursuant to the provider participation agreement; and

    d. As required by applicable law.

    If BA discloses PHI to a third party for a permitted reason under Section 1(a) or 1(b) above, BA shall ensure that reasonable assurances are obtained from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it

was disclosed to such person and that the person notifies BA of any instances of which it is aware in which the confidentiality of the information has been breached;

BA shall not knowingly use or disclose PHI in a way that would violate the Privacy Rule or Security Rule.

To the extent practicable, BA shall use a Limited Data Set (as defined in the Privacy Rule) with respect to PHI of Company. If not practicable, BA shall use the least amount of PHI necessary to achieve the intended purpose. BA shall comply with any guidance issued by the Secretary of the United States Department of Health and Human Service (the "Secretary") regarding the minimum necessary use and disclosure of PHI.

BA shall not sell, nor directly or indirectly receive remuneration for the use and disclosure of, PHI, except as otherwise authorized by the applicable individual(s) or otherwise permitted by HIPAA.

2. Comply with the Security Rule, including without limitation, 45 CFR 164.306 (general obligations), 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards), 164.314 (contracts with subcontractors) and 164.316 (implementing policies and procedures to comply with the Security Standards).

3. Report to the Company who provided such PHI any use or disclosure of PHI not provided for by this Agreement of which BA becomes aware, including any security incident as described in the Security Rule.

   BA agrees to cooperate with the Company as it determines whether any such impermissible use or disclosure of PHI constitutes a breach of unsecured PHI for purposes of 45 CFR §164.400 *et seq.* and whether such breach requires notification by the Company to individuals, the media, and/or the Secretary.

   In furtherance of the foregoing, in the event BA discovers a breach of PHI, BA agrees:

   i. To provide the Company with relevant information, including a brief description of the incident, the date of the incident, the individuals potentially affected, the date of discovery, the type of PHI involved, and any recommendations that should be made to individuals for their protection.

   ii. To reasonably cooperate and coordinate with the Company to further investigate any breach incident, to assist in making notifications to individuals as necessary, and to mitigate, to the extent practicable, any harm resulting or that may result from a breach incident.

4. Ensure that any of its agents or subcontractors to which BA provides PHI received from or created or received on behalf of the Company agrees to the same restrictions and conditions that apply through this Agreement to BA with respect to PHI. In furtherance of the foregoing, BA shall ensure that any of its agents or subcontractors that create, receive, maintain or transmit EPHI on behalf of BA agree to comply with the applicable requirements of the Security Rule by entering into a contract or other arrangement that complies with 45 CFR §164.314.

5. To the extent BA maintains PHI in a designated record set (as defined by HIPAA and implementing regulations) and at the request of the Company, make such PHI available for access to the Company except for:

   a. PHI maintained by BA which is a copy of PHI held by the Company; or

   b. Information that is protected by the Privacy Rule or other applicable law from disclosure.

6. To the extent BA maintains PHI in a designated record set (as defined by the Privacy Rule) and at the request of the Company, make available to the Company such PHI for amendment and incorporate any amendments to PHI provided by the Company.

7. Document disclosures of PHI and information related to such disclosures, and at the request of the Company, provide documentation of disclosures of PHI made by BA and provide the following information related to each such disclosure for purposes of enabling the Company to provide an accounting of

disclosures of PHI as required under the Privacy Rule:

a. The date of the disclosure;

b. The name of the entity or person who received PHI and, if known, the address of such entity or person;

c. A brief description of PHI disclosed; and

d. A brief statement of the purpose of the disclosure that reasonably informs the Company of the basis for the disclosure.

The foregoing is subject to all of the exceptions to an accounting of disclosures of PHI provided in the Privacy Rule (*e.g.*, no accounting is required for disclosures of PHI made in connection with health care operations as defined by the Privacy Rule).

8. Make its internal practices, books, and records relating to the use and disclosure of PHI received from or by BA on behalf of the Company available to the Secretary for purposes of determining the Company's compliance with the Privacy Rule and the Security Rule.

9. To the extent BA is to carry out Company's obligations under the Privacy Rule, BA shall comply with the requirements of the Privacy Rule that apply to Company in the performance of such obligations.

10. BA shall comply with any restrictions on the disclosure of PHI requested by an individual and agreed to by Company and of which BA has notice.

11. Each party hereto is responsible for determining its own compliance with HIPAA and its implementing regulations.

Obligations of Company

The Company shall:

1. Not request BA to use or disclose PHI in any manner that would not be permissible under the Privacy Rule or the Security Rule if done by the Company.

2. Notify BA of any changes in, or revocation of, permission by an individual to use or disclose PHI, to the extent that such changes may affect BA's use or disclosure of PHI.

3. Notify BA of any limitations in or changes to its Notice of Privacy Practices to the extent that such limitation or change may affect BA's use or disclosure of PHI.

4. Notify BA of any restriction on the use or disclosure of PHI that it has agreed to in accordance with the Privacy Rule to the extent that such restriction may affect BA's use or disclosure of PHI.

5. At all times comply with the Privacy Rule's standards relating to minimum necessary use and disclosure of PHI. Company will avoid transmitting or otherwise communicating PHI to BA except in accordance with the Privacy Rule's standards relating to minimum necessary use and disclosure of PHI.

Material Breach Involving PHI

Upon the Company's knowledge of a material breach by BA of the provisions of this Agreement involving the use or disclosure of PHI, the Company shall provide BA with written notice of such breach, including a description of the breach. The Company shall provide BA with an opportunity to cure by taking steps to change such circumstances within the sixty-day period following the notice. If the breach is not cured within such sixty-day period, the Company may terminate this Agreement, if feasible. BA acknowledges that if termination under those circumstances is not feasible, the Company is obligated to report the violation to the Secretary of the United States Department of Health and Human Services.

In the event BA learns of a pattern of activity or practice by the Company of material breach or violations of the terms and conditions set forth herein, if the Company fails to cure or end such breach or violations, BA shall have the right to terminate this Agreement, or if termination is not feasible, report the material breach or violations to the Secretary.

Effect of Termination or Cancellation

BA and the Company acknowledge that PHI will be needed by BA following the termination or cancellation of the Agreement for purposes described herein, and that it therefore is not feasible for BA to return or destroy all PHI received from or on behalf of the Company. Therefore, BA shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return infeasible for so long as BA maintains such PHI. These provisions shall survive termination of this Agreement.

Amendment

The parties agree to take such action as is necessary to amend this Agreement from time to time as necessary to comply with HIPAA and implementing regulations and guidance.

In witness whereof, the parties have executed this Business Associate Agreement on the 4th day of October, 2018.

JOINT VENTURE HOSPITAL **BUSINESS ASSOCIATE**

By: _____ By: _____

Its: Chief Executive Officer Its: _____

Date: _____ Date: _____

N0177531.DOCX

Sample Business Associate Checklist for Evaluating HIPAA Compliance

Business Associate Security Questionnaire

JVHL has identified you as a Business Associate. In order to be compliant with the HIPAA Security Rule due diligence requirement to evaluate the safeguards of Protected Health Information (PHI) please complete this HIPAA/HITECH security questionnaire in lieu of a full security assessment.

Business Associate Name: _____ Date: _____
Primary Contact Name: _____ Title: _____
Phone: _____ Fax: _____ E-mail: _____

What type of services do you provide to JVHL and how is PHI used, accessed, disclosed, transmitted and/or stored? _____.

Administrative Safeguards
Do you keep an inventory of where PHI is used, disclosed, stored, and transmitted to? _____
If yes, what was the date of the latest inventory? _____
When was the last risk analysis conducted? _____
Have identified risks been mitigated or formally accepted? _____
When was the last compliance assessment/evaluation conducted? _____
Have identified compliance issues been mitigated _____
Has a formal contingency plan been adopted? _____
When was the last update? _____
Is ePHI stored or accessed on portable media? _____
If yes, describe your security measures taken to protect ePHI and attach policies:

_____

What was the date of your last full back up performed? _____
How often do you perform full back ups? _____
Is your back up stored off site? _____
Is your back up encrypted? _____
Has a formal disaster recovery plan been adopted? _____
Describe your process or attach the policy and/or form to grant workforce members' access to PHI? _____
Describe your process or attach the policy and/or form to terminate workforce members' access to PHI and facilities? ____
_____
Please provide the date employees and management underwent security training?_____
_____
Were the applicable HITECH Act requirements included in the training? _____ (such as security incident response and breach investigation information)
Please attach a description of all security testing that has been performed over the past year.

Physical Safeguards
Please describe your measures to destroy items containing PHI (media, paper, hard drives)? _____
_____
Do you allow personal devices to be connected to the same network which contains ePHI? _____
_____
If so, are the personally owned mobile devices approved and secure? If so, how are the mobile devices secured? _____
_____
_____
Attach policies or describe security measures in place to prevent unauthorized physical access, tampering, and theft of ePHI.

Technical Safeguards
Please provide your password policy or describe how passwords are required for all applications that provide access to ePHI. _____
Do your systems automatically terminate after a period of inactivity? _____ If so, what is the time frame? _____.
Do users have unique accounts to access ePHI? _____.
Do you grant users local administrative rights on their workstations? _____.
Do you use a wireless network? _____. If yes, what measures do you have in place to secure ePHI? _____.
Do you send ePHI outside your network? _____
If yes, what measures do you have in place to protect ePHI sent outside your network?
_____
_____
Do you have a central repository for security events from applications, systems, and/or network devices? _____.
If yes, when was the date they were last reviewed? _____
How often are they reviewed? _____

Breach Notification
Please provide your security incident response and breach notification policies.
Have you appointed a security incident response team? ____
Have you developed a security incident response plan? ____ If yes, when was the plan last tested? _____
Do you send ePHI outside your network? _____ If yes, what measures do you have in place to protect ePHI sent outside your network?
_____
Third Party Vendors
Do you use any third party vendor that uses, discloses, transmits or stores PHI? _____

Third party vendor(s). (name): _____ **Contact Number:** _____
Has a formal contract been executed with the third party vendor requiring the vendor comply with the HIPAA/HITECH Act privacy and security standards? _____
If so, how do you check your third-party vendor's security measures? _____
What was date of the last time you checked the third-party vendor's security measures? _____

Who is the third-party vendor's HIPAA security contact? _____
Phone: _____

Third party vendor(s). (name): _____ **Contact Number:** _____
Has a formal contract been executed with the third party vendor requiring the vendor comply with the HIPAA/HITECH Act privacy and security standards? _____
If so, how do you check your third party vendor's security measures? _____ What was date of the last time you checked the third-party vendor's security measures? _____
Who is the third-party vendor's HIPAA security contact? _____
Phone: _____

Please send the questionnaire to:
Joint Venture Hospital Laboratories
Attn: JVHL Security Officer
999 Republic Dr., Suite 300
Allen Park, MI 48101

Documentation Provided By:
Signature _____ Date _____
Printed Name _____
Title _____

Documentation Reviewed By:
Signature _____ Date _____
Printed Name _____
Title _____

Follow up Audit Required: (Y) (N)

Privacy Officer Job Description

Position Title: Privacy Officer

Immediate Supervisor: Chief Executive Officer

Position Overview: **Under HIPAA (the Health Insurance Portability and Accountability Act of 1996) every healthcare organization must designate a privacy official.** The privacy official may have other titles and duties in addition to his/her privacy official designation in a typical Office or organizational setting. In terms of HIPAA compliance, the Privacy Officer function is responsible for overseeing all ongoing activities related to the development, implementation, maintenance, and adherence to the organization's policies and procedures covering the privacy and access of patient health information in compliance with federal and state laws and healthcare organizations' information privacy practices.

General Purpose: The Privacy Officer function is responsible for overseeing all ongoing activities related to the development, implementation, maintenance, and adherence to the organization's policies and procedures covering privacy, access, and patient health information in compliance with federal and state laws and healthcare organizations' information privacy practices.

The position accomplishes this through a respectful, constructive and energetic style, guided by the objectives of the company.

Privacy Roles and Responsibilities

- Provides development guidance and assists in the identification, implementation, and maintenance of organization information privacy policies and procedures in coordination with leadership and legal counsel.
- Performs periodic privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions
- Establishes with leadership a mechanism to track access to protected health information as required by law
- Reviews all system-related information security plans throughout the organization to ensure alignment between security and privacy practices and acts as a liaison to the information systems department
- Ensures proper response to occurrences of breach and reporting of violations or potential violations to duly authorized enforcement agencies as appropriate and/or required
- Oversees, directs, delivers, or ensures delivery of privacy training and orientation to all employees
- Assist Chief Executive Officer in representing JVHL to the third-party payers and providers as it relates to privacy
- Assist Chief Executive Officer with our corporate legal counsel as it relates to developing and finalizing contract language around privacy.

Other Roles and Responsibilities

- Advise JVHL Leadership on issues related to areas of responsibility
- Serve as a member of the JVHL Leadership Team
- Contribute to other areas and perform duties at JVHL as needed
- Update job knowledge by participating in education opportunities
- This position will require access to Patient Health Information (PHI), both electronic and hardcopy, so employees will be required to assist in its protection by following corporate policies and procedures that are designed to maintain the privacy and security of PHI.

Education/Qualifications:

- Baccalaureate degree in healthcare administration, public health, law, or a related healthcare field.
- Knowledge and experience in compliance and privacy laws and regulations

- Recommended compliance certification in Compliance & Ethics Professional (CCEP) or Certified in Healthcare Compliance (CHC)
- Recommended privacy certification such as Healthcare Privacy and Security (CHPS) and/or other healthcare industry related credentials, e.g. RHIA, RHIT.

Preferred Skills:

- Experience with credentialing
- Working knowledge of NCQA certification
- Aptitude in decision making, problem solving, project management, and thoroughness
- Outstanding interpersonal, organizational and leadership abilities
- Proficient in computer skills including Microsoft Word, Excel, PowerPoint, and Outlook
- Excellent verbal and written communication skills
- Change Agent
- Ethical Conduct