JotForm HIPAA Compliance

Learn how JotForm not only complies with HIPAA, but builds a better, more secure environment to mitigate your risk and help you prove compliance with HIPAA. We did the hard work so you don't have to, and you can inherit a lot of the work that we've done in terms of audits. Our HIPAA-compliant API, platform, and data integration service simplify compliance for you. To learn more about our products or to get set up with an account today, visit https://www.jotform.com/hipaa/. In an effort to be transparent, we go into a good amount detail on this page. As a lead in, below is a high level summary of our major architecture, our guiding principles, and how it maximizes our security.

Need	JotForm Approach
Encryption	All data is encrypted in transit, end to end, and at rest. Log data is also encrypted to mitigate risk of ePHI stored in log files.
Minimum Necessary Access	Access controls are always defaults to no access unless overridden manually.
System Access Tracking	All access requests and changes of access, as well as approvals, are tracked and retained.
PHI Segmentation	All customer data is segmented. Additionally, all platform customers have a dedicated overlay network (subnet) for additional network segmentation.
Monitoring	All network requests, successful and unsuccessful, are logged, along with all system logs. API PHI requests (GET, POST, PUT, DELETE) log the requestor, location, and

	data changed/viewed. Additionally, alerts are proactively sent based on suspicious activity. OSSEC is used for IDS and file integrity monitoring.
Auditing	All log data is encrypted and unified, enabling secure access to full historical network activity records.
Minimum Risk to Architecture	Secure, encrypted access is the only form of public access enabled to servers. All API access must first pass through JotForm AWS firewalls. To gain full access to JotForm systems, users must login via 2 factor authentication through VPN, authenticate to the specific system as a regular user, and upgrade privileges on the systems temporarily as needed.
Vulnerability Scanning	All customer and internal networks are scanned regularly for vulnerabilities.
Intrusion Detection	All production systems have intrusion detection software running to proactively detect anomalies.
Backup	All customer data is backed up every 24 hours. Seven (7) days of rolling backups are retained.
Disaster Recovery	JotForm has an audited and regularly tested disaster recovery plan. This plan also applies to customers, and they inherit this from us.
Documentation	All documentation (policies and procedures that make up our security and compliance program) is stored and versioned using Google Docs.

Risk Management	We proactively perform risk assessments to assure changes to our infrastructure do not expose new risks to ePHI. Risk mitigation is done before changes are pushed to production.
Workforce Training	Despite not having access to the ePHI of our customers, all JotForm workforce members undergo HIPAA and security training regularly.

See the details of how we comply with HIPAA below. These are mapped to specific HIPAA rules. There's a lot here but again, we are taking on this responsibility so that our customers don't have to. Controls marked with an (Req) are *Required*. Controls marked with an (A) are *Addressable*. In our environment, controls outlined below are implemented on all infrastructure that processes, stores, transmits, or can otherwise gain access to ePHI (electronic protected health information).

Administrative Safeguards (see 164.308)

Taken directly from the wording of the Security Rule, administrative safeguards are *administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.*
There aren't specific security settings in this section, and the most important area covered is the risk assessment. The risk assessment is a fundamental process for any organization that wants to become compliant.

Security Management Process - 164.308(a)(1)(i)

Standard	Description
Risk Analysis (Req)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity.
Risk Management (Req)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec. 164.306(a) [Security standards: General rules; (a) General requirements].
Sanction Policy (Req)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
Information System Activity Review (Req)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

JotForm has a risk management policy that defines the risk analysis and risk management process. This policy is operationalized with processes to conduct regularly risk assessments. JotForm uses NIST800-30 and 800-26 for performing risk analysis. Our policy begins with an inventory of all JotForm systems, mapping of where ePHI is processed, transmitted, or stored, identification of threats, risks, and likelihood, and the mitigation of risks. Policies address risk inherent within the environment and mitigating the risk to an acceptable and reasonable level.

JotForm has a Sanction Policy that has sanctions for employees not adhering to certain policies, and for specifically violating HIPAA rules.

Policies and procedures address the requirements of monitoring and logging system level events and actions taken by individuals within the environment. All requests into and out of the JotForm network are logged, as well as all system events. JotForm, has implemented multiple logging and monitoring solutions to track events within their environment and to monitor for certain types of behavior. Log data is regularly reviewed. Additionally, proactive alerts are enabled and triggered based on certain suspicious activity.

Assigned Security Responsibility - 164.308(a)(2)

Standard	Description
Assigned Security Responsibility (Req)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

JotForm has formally assigned and documented its security officer. Our security officer is Uygar Bayar. He can be reached by email at uygar [at] jotform.com.

Workforce Security - 164.308(a)(3)(i)

Standard	Description
Authorization and/or Supervision (A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

Workforce Clearance Procedure (A)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
Termination Procedures (A)	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [Workforce Clearance Procedures] of this section.

JotForm has policies in place that require workforce members requesting access to ePHI to submit an authorization form that is signed and acknowledges their responsibility of safeguarding ePHI. The form must also be approved by the Security Officer. Once signed and approved, then the individual will be provisioned access to systems deemed business necessary. All Access to ePHI is based on minimum necessary requirements and least privilege. JotForm cannot access ePHI unless customers explicitly grant access.

JotForm policies define the immediate removal of access once an employee has been terminated, with the Security Officer responsible for terminating the access. Once HR initiates the termination process the termination checklist is referenced to ensure necessary actions are taken to remove systems and facilities access.

Information Access Management - 164.308(a)(4)(i)

Standard	Description
Isolating Health care Clearinghouse Function (Req)	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
Access Authorization (A)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
Access Establishment and Modification (A)	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

JotForm does not perform the functions of a Healthcare Clearinghouse, so aspects of this section are not applicable.

The Security Officer determines the roles necessary for each system and application. When access is needed to JotForm infrastructure, a request and acknowledgement form is signed and then approved by the Security Officer.

JotForm has a formal process for requesting additional access to ePHI, and again JotForm customers must approve all requests concerning ePHI.

Security Awareness and Training - 164.308(a)(5)(i)

Standard	Description
Security Reminders (A)	Periodic security updates to all members of JotForm
Protection from Malicious Software (A)	Procedures for guarding against, detecting, and reporting malicious software.
Log-in Monitoring (A)	Procedures for monitoring login attempts and reporting discrepancies.
Password Management (A)	Procedures for creating, changing, and safeguarding passwords.

JotForm has a Security Awareness training policy in place that requires new employees and current employees to conduct training upon hire and annually thereafter. Minimum training is done annually, with regular informal security and compliance training done every other week.

JotForm proactively assesses and tests for malicious software within their environment, both infrastructure and workstations. Members of the JotForm team monitor bug and vulnerability lists to assure they remain up to date.

JotForm is monitoring and logging successful and unsuccessful login attempts to the servers within its environment and policies are in place requiring audit logging, which include login attempts.

Password configurations are set to require that passwords are a minimum of 8 characters in length and have a 90-day password expiration, account lockout after 5 invalid attempts, password history of last 6 passwords remembered, and an account lockout after 15 minutes of inactivity.

Security Incident Procedures - 164.308(a)(6)(i)

Standard	Description
Response and Reporting (Req)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

JotForm has implemented a formal incident response plan (IRP), which discusses the procedures for identifying, responding to, and escalating suspected and confirmed security breaches. JotForm has implemented an incident response team for the purposes of dealing with potential security breaches. The IRP has specific types of incidents to look out for, as well as some common types of incidents that are monitored for within the environment.

Contingency Plan - 164.308(a)(7)(i)

Standard	Description
Data Backup Plan (Req)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
Disaster Recovery Plan (Req)	Establish (and implement as needed) procedures to restore any loss of data.
Emergency Mode Operation Plan (Req)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.

Testing and Revision Procedure (A)	Implement procedures for periodic testing and revision of contingency plans.
Applications and Data Criticality Analysis (A)	Assess the relative criticality of specific applications and data in support of other contingency plan components.

JotForm has a formal Backup and Recovery Policy that defines the data backup strategy, including: schedule, associated responsibilities, and any risk-assessed exclusion to the backup schedule.

JotForm has a formal Disaster Recovery plan to ensure the efficient recovery of critical business data and systems in the event of a disaster. The DR plan includes specific technical procedures necessary to reinstate the infrastructure and data to allow critical business functions to continue business operations after a disaster has occurred. Additionally, the JotForm DR plan includes requirements for performing annual testing of the DR plan to ensure its effectiveness.

JotForm has a DR plan, or a Business Continuity Plan (BCP), to aid in the efficient recovery of critical business functions after a disaster has been declared. The BCP goes into effect after facility outage of 24 hours. The BCP identifies critical information necessary to resume business operations such as: Hardware/software requirements, recovery time objectives, forms, employee/vendor contact lists, alternate working procedures, emergency access procedures, and a data and application criticality analysis. The BCP includes an Emergency Mode Operations Plan that addresses the access and protection of ePHI while operating in emergency mode.

The DR and BPC plans are reviewed and tested annually or whenever significant infrastructure changes occur.

JotForm has a performed an applications and data criticality analysis that details what systems and application need be recovered and their specific order in the recovery process.

Evaluation - 164.308(a)(8)

Standard	Description
Evaluation (Req)	Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic PHI that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

JotForm has formal internal policies and procedures for conducting periodic technical and non-technical testing. These define procedures for performing quarterly internal and external vulnerability scanning, as well as annual penetration testing. Vulnerability scanning is performed regularly on a weekly basis and with any major changes in infrastructure. Additionally, non-technical evaluations occur on an annual basis to ensure that the security posture of JotForm is at the defined level, approved by management, and communicated down to JotForm employees.

Business Associate Contracts and Other Arrangement - 164.308(b)(1)

Standard	Description
Written Contract or Other Arrangement (Req)	A covered entity, in accordance with Â§ 164.306 [Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Â§ 164.314(a) [Business Associate Contracts or Other Arrangements] that the business associate will appropriately safeguard the information. Document the satisfactory assurances required by paragraph (b)(1) [Business Associate

	Contracts and Other Arrangements] of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of Â§ 164.314(a) [Business Associate Contracts or Other Arrangements].

JotForm has a formalized template, as well as policies in place regarding Business Associate Agreements (BAA) and written contracts. JotForm has engaged a third-party provider for hosting responsibilities and has written attestations of safeguarding its data. Additionally, JotForm performs due diligence in assuring that third-party providers they select go through their due diligence process and provide services consistent with JotForm's security and compliance posture.

Physical Safeguards (see 164.310)

This one is pretty straight forward - *physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.* Data center security is typically easier to address than office security, though at JotForm we address both.

Facility Access Controls - 164.310(a)(1)

Standard	Description
Contingency Operations (A)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
Facility Security Plan (A)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Access Control and Validation Procedures (A)	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
Maintenance Records (A)	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

JotForm infrastructure supporting its environments is hosted at AWS (Amazon Web Services) which provides hosting and recovery services for the infrastructure.

The JotForm headquarters also has written policies and procedures for safeguarding the corporate location, which include workstations with access to the environment protected from unauthorized physical access. The JotForm environment is entirely hosted and built on hardware components provided by AWS which JotForm would never have access into.

Workstation Use - 164.310(b)

Standard	Description
Workstation Use (Req)	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

JotForm has policies in place that define the acceptable uses in place for workstations within the environment. These policies define the acceptable and unauthorized uses of personnel that provide workstations with access to systems potentially interacting with ePHI. These policies are enforced on all workstations. All internal email uses HIPAA-compliant vendors.

Workstation Security - 164.310c

Standard	Description
Workstation Security (Req)	Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

JotForm has a formal Workstation and Portable Media Security Policy that identifies the specific requirements of each device. The policies define the requirements for using and/or restricted specific actions while engaged with any ePHI. Additionally, workstations are secured appropriately to limit exposure to breaches. Actions and events are monitored and controlled, with user restrictions on downloading or copying any ePHI without documented approval and business justification. Additionally, all file storage internally at JotForm utilizes HIPAA-compliant cloud-based vendors (currently AWS S3 and Google Apps).

Device and Media Controls - 164.310(d)(1)

Standard	Description
Disposal (Req)	Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.
Media Re-use (Req)	Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.
Accountability (A)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Data Backup and Storage (A)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

JotForm has policies and procedures for all workstations that interact with and may potentially become exposed to ePHI. These policies have requirements for secure media disposal so that ePHI cannot be recovered from these systems.

JotForm has Media re-use requirements for the workstations, despite the fact that these workstations do not have access to and interaction with ePHI.

Technical Safeguards (see 164.312)

This section of HIPAA outlines *the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.* It is important to note that these requirements are not prescriptive, and there is flexibility in implementation. The key is that measures that are reasonable and appropriate are implemented to safeguard ePHI.

Access Control - 164.312(a)(1)

Standard	Description
Unique User Identification (Req)	Assign a unique name and/or number for identifying and tracking user identity.
Emergency Access Procedure (Req)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
Automatic Logoff (A)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Encryption and Decryption (A)	Implement a method to encrypt and decrypt electronic protected health information.

All users within the JotForm environment are issued a unique username and password. All accounts are local and unique. General/shared accounts are not in place and root access is restricted and monitored.

JotForm has a process for obtaining access to ePHI should an emergency or disaster occur. JotForm systems settings on all of its servers have session timeout features enabled and configured to terminate sessions after 30 minutes.

JotForm encrypts all stored data in its environment using 256-bit AES encryption. Additionally, all data in transit is encrypted end to end (more below).

Audit Controls - 164.312(b)

Standard	Description
Audit Controls (Req)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

JotForm has policies in place addressing audit trail requirements. Systems within the its environment are logged to a centralized logging solution, AWS S3, which monitors system level events and contains a user ID, timestamp, event, origination, and type of event. These logs are constantly monitored for suspicious events and alerts are generated for any type of behavior that is suspicious.

Integrity - 164.312c(1)

Standard	Description
Mechanism to Authenticate Electronic Protected (A)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

JotForm has employed a centralized access control system for authenticating and accessing internal systems where ePHI resides. Currently, JotForm employees access a bastion host using an SSH-2 connection to access internal systems. Accounts on the internal database are restricted to a limited number of personnel, with logging in place to track all transactions.

Person or Entity Authentication - 164.312(d)

Standard	Description
Person or Entity Authentication (Req)	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

JotForm has a formal policy that describes the process of verifying a person’s identity before unlocking their account, resetting their password, and/or providing access to ePHI.

Transmission Security - 164.312(e)(1)

Standard	Description
Integrity Controls (A)	Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection.

Encryption (A)	Implement a mechanism to encrypt ePHI in transit.

All data in transit with JotForm is sent over internet connections through an TLS1.1/TLS1.2 encrypted mechanism. Load balancers segment the traffic and send transmissions of the data to the application servers via an encrypted connection using the TLS protocol. Additionally, none of the internal application servers, database servers, and log and monitoring servers are accessible via public internet. All internal servers must be accessed through a bastion host which is not accessible from the internet and require an SSH connection.

Organizational Requirements (see 164.314)

These requirements simply outline the need for a business associate agreement (BAA) between covered entities and business associates. This requirement has recently been extended to require a BAA between business associates and all subcontractors. That linking, chaining together of a BAA, has created for new and interesting legal and business questions. Basically, each layer in the chain of BAA takes on certain responsibilities and certain risks as part of HIPAA, and there needs to be consistency. Case in point, at JotForm we have several customers that have moved over from compliant IaaS providers because those providers had breach notification timelines that were not acceptable for large healthcare enterprises. We've taken a proactive approach to BAA to mitigate risk for our customers and assure consistency along the chain of BAA.

Business Associate Contracts or Other Arrangements - 164.314(a)(1)(i)

Standard	Description

Business Associate Contracts (Req)	The Implementation Specifications for the HIPAA Security Rule Organizational Requirements “Business Associate Contracts or Other Arrangements” standard were evaluated under section 164.308(b)(1) above.
Other Arrangements (Req)	Rules to engaging with additional 3rd parties, like subcontractors.

JotForm has a formalized policy and process is in place concerning the BAA. A BAA templates is in place and BAA contracts are reviewed for consistency. JotForm has a formal policy and process in place for performing due diligence with any third party or vendor before engaging them. Additionally, contracts are retained that detail the responsibility of safeguarding any information to which the provider may have access, as well as creating consistency for JotForm and JotForm customers.

Policies and Procedures and Documentation Requirements (see 164.316)

Policies and Procedures - 164.316(a)

Standard	Description
Policies and Procedures (Req)	Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in Â§ 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart.

JotForm has a formalized Policy Management program that ensures that policies are developed, implemented, and updated according to best practice and organization requirements. In the words of our auditors, this is a policy about our policies.

Documentation - 164.316(b)(1)(i)

Standard	Description
Time Limit (Req)	Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
Availability (Req)	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
Updates (Req)	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

JotForm retains the necessary policies and documentation for a minimum of 6 years. All policies and procedures are available and distributed to personnel on the company's shared drive (currently Google Docs). JotForm has an update and review process for reviewing all policies and procedures and updating them as necessary. Additionally, JotForm tracks and maintains revision history, approval signature, and timestamps to ensure policies are reviewed and updated according to organization requirements.

HITECH Act and Omnibus Rule: IT Security Provisions

These were updates made to strengthen the Privacy, Security, and Breach Notifications rules within HIPAA. These updates went into effect in 2013 and were the driving force for many existing IaaS vendors to begin signing BAAs.

Notification in the Case of Breach - 13402(a) and 13402(b)

Standard	Description
In General	A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.
Notification of Covered Entity by Business Associate	The requirements for the HITECH Act Notification in the Case of Breach - Notification of Covered Entity by Business Associate - Uses and Disclosures: Organizational Requirements “Business Associate Contracts” standard are located in the “BA Requirements” worksheet.

JotForm has a formal breach notification policy that addresses the requirements of notifying affected individuals and customers of a suspected breach of ePHI. These policies outline the relevant and responsible parties in case of a breach, forensics work to discover extent of breach, reason for breach, correction of infrastructure to prevent any future breach, and requirements for notifying customers of a breach within 24 hours. JotForm is a defined Business Associate or subcontractor according to HIPAA regulations and the specific customer relationship.

Timeliness of Notification - 13402(d)(1)

Standard	Description
In General	Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved (or business associate involved in the case of a notification required under subsection (b)).

JotForm has a breach notification policy that addresses the requirements of notifying the affected individuals or customers within 24 hours of a breach.

Content of Notification - 13402(f)(1)

Standard	Description
Description of Breach	Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following: (1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
Description of EPHI Involved	(2) A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
Actions by Individuals	3) The steps individuals should take to protect themselves from potential harm resulting from the breach.
Contact Procedures	(5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

JotForm has Breach Notification policies in place and they include a brief description of the breach, including the date of the breach and the date of the discovery of the breach, if known. JotForm breach notification policies include a description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of personally identifiable information were involved) and what the source of the breach was. Our breach

notification policies include steps the individual should take to protect themselves from potential harm resulting from the breach. Our policies also provide the contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or postal address.