DNAnexus HIPAA Compliance Mapping v1.1 20140620

HIPAA (45 CFR)	HIPAA Specifications	ISO 27002:2005 Reference	DNAnexus Provides	Customer Responsibility on the DNAnexus Platform
Security Rule - Administrative Safeguards				
§164.308(a)(1)(ii)(A)	Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	5.1 INFORMATION SECURITY POLICY	DNAnexus performs annual Risk Assessments under an ISO 27001 Information Management System. The assessements are compatible with NIST 800-30 standard guide for conducting risk assessments. During the Risk Assessment we classify Assets, Threats, and Vulnerabilities, and rate Risks	
§164.308(a)(1)(ii)(B)	Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	5.1 INFORMATION SECURITY POLICY	DNAnexus has implemented an ISO 27001 Information Management System (ISMS). We create risk treatment plans based on prioritized identified risks, and manage implementation of the risk treatment plans. DNAnexus Risk Treatment plans identify planned dates for acceptable mitigation. Additionally, sub-tasks are tracked in a ticketing system and assigned owners and completion timeframes.	
§164.308(a)(1)(ii)(C)	Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	5.1 INFORMATION SECURITY POLICY	DNAnexus' official Human Resources Security Policy requires adherence to security policies, and violation of these policies is punishable by discipline up to and including termination.	
§164.308(a)(1)(ii)(D)	Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	5.1 INFORMATION SECURITY POLICY	Logs and reports are reviewed regularly. The Incident Response plan is tested and reviewed annually. Identified anomalies and incidents are tracked in a ticketing system until resolved.	Periodically review access to your Projects.
§164.308(a)(2)	Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	6.1.3 Allocation of information security responsibilities	Roles and responsibilities are clearly identified in security policies and procedures.	
§164.308(a)(3)(ii)(A)	Authorization and/or supervision (Addressable). 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.	8 HUMAN RESOURCES SECURITY	background check to verify employment and academic history and to also check for felony convictions Production access is limited to a few administrators, and their activities are monitored with both technical and managerial controls.	
§164.308(a)(3)(ii)(B)	Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	8 HUMAN RESOURCES SECURITY	All access is approved.	Determine whether access to your Projects is appropriate.
§164.308(a)(3)(ii)(C)	Termination procedures (Addressable). 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) of this section.	8 HUMAN RESOURCES SECURITY	Documented termination procedures require revocation of access within one day of termination or re-assignment.	
§164.308(a)(4)(ii)(A)	Isolating health care clearinghouse functions (Required). 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.	11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL 11.2 USER ACCESS MANAGEMENT	DNAnexus is not a Health Care Clearinghouse, and is not a Covered Entity. DNAnexus is a Business Associate, and processes potential health data according to agreements and instructions from DNAnexus' customer.	
§164.308(a)(4)(ii)(B)	Access authorization (Addressable). 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.	DNAnexus CONFIDENTIAL specification	Customer access to the DNAnexus platform is managed with individual accounts and passwords. DNAnexus administrative access to the production system is managed with individual accounts and two-factor authentication. Project Administrators may specify "Copy Not Allowed" to prevent non-administrators from moving data to other projects. Production access is highly limited and is approved and reviewed by management.	Designate platform Project owners, to grant and manage access to your data. If appropriate, anonymize sequence data prior to uploading it to the Site, and do not include personally identifiable information in tags, file names, file data, project names, or other locations. Use the "Copy Not Allowed" project setting when appropriate.
§164.308(a)(4)(ii)(C)	Access establishment and modification (Addressable). 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.	(Disclosed under NDA only)	All production-related accounts are formally reviewed periodically. User account access to projects is granted by a Project Administrator, who can specify Viewer, Uploader, Contributor, or Administrator roles for other users.	Grant appropriate access to your Projects, using the DNAnexus project roles, and periodically review user rights.
§164.308(a)(5)(ii)(A)	Security reminders (Addressable). Periodic security updates.	8.2.2 Information security awareness, education, and training 11.3.1 Password use	DNAnexus conducts annual security awareness training for all employees.	
§164.308(a)(5)(ii)(B)	Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.	8.2.2 Information security awareness, education, and training 11.3.1 Password use	All workstations commonly affected by malicious software are protected with anti-malware. Signatures and engines are automatically and regularly updated.	Protect workstations used to access the DNAnexus platform with appropriate anti-malware.
§164.308(a)(5)(ii)(C)	Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	8.2.2 Information security awareness, education, and training 11.3.1 Password use	Attempts (successful and unsuccessful) to log in to Production system administration are logged and reviewed by Security Operations personnel.	

§164.308(a)(5)(ii)(D)	Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.	8.2.2 Information security awareness, education, and training 11.3.1 Password use	PHI Customer account passwords are required to be complex and to be changed regularly. DNAnexus can customize these settings to customer policies. DNAnexus administration passwords are protected with two-factor authentication.	Safeguard your DNAnexus passwords, and do not share them with anyone.
§164.308(a)(6)(ii)	Implementation specification: Response and Reporting (Required). 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.	13 INFORMATION SECURITY INCIDENT MANAGEMENT	DNAnexus has a documented Incident Response Plan which is tested and reviewed annually. Security Incidents are handled according to the Incident Response Plan, which included investigation and tracking in the ticketing system, and external parties are notified according to the Plan	
§164.308(a)(7)(ii)(A)	Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	14 BUSINESS CONTINUITY MANAGEMENT	Data and backups are stored in Amazon S3, which provides triple-redundant storage immediately upon saving. Databases are run in redundant clusters, and also backed up daily. All transfers to and from S3 are encrypted with HTTPS. Projects can be marked as "Delete Not Allowed" to prevent anyone but the Project Administrator from deleting data to prevent accidental data deletions. Amazon S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year.	Delete data only when appropriate. Use "Delete Not Allowed" project settings as needed. If appropriate, download and archive additional data backups.
§164.308(a)(7)(ii)(B)	Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.	14 BUSINESS CONTINUITY MANAGEMENT	DNAnexus has formal Disaster Recovery and Backup Procedures, and reviews these plans periodically. Amazon's Business Continuity Management has been certified to ISO 27001 standards.	
§164.308(a)(7)(ii)(C)	Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	14 BUSINESS CONTINUITY MANAGEMENT	Amazon provides a high level on continuity for AWS services and Amazon's IT Business Continuity Plans. DNAnexus can continue to provide service as long as AWS services are available - there are no external dependencies for emergency mode operation. Amazon's Business Continuity Management has been certified to ISO 27001 standards.	
§164.308(a)(7)(ii)(D)	Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.	14 BUSINESS CONTINUITY MANAGEMENT	DNAnexus does periodic testing of DR/BC plans. Amazon's Business Continuity Management has been certified to ISO 27001 standards.	
§164.308(a)(7)(ii)(E)	Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.	14 BUSINESS CONTINUITY MANAGEMENT	As part of the annual Risk Analysis, DNAnexus identifies mission critical systems, databases, and applications. DNAnexus has prioritized criticality and risk, and considered the relationship of applications and data to contingency planning. Amazon's Business Continuity Management has been certified to ISO 27001 standards.	
§164.308(a)(8)	Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE	DNAnexus undergoes an annual third-party validation of technical and procedural security under the ISO 27001 certification process. The last report validating compliance was completed 1/29/2014. In accordance with the ISO 27001 ISMS, DNAnexus has implemented and documented both Corrective and Preventive actions triggered by incidents, audits, and desired improvements.	
§164.308(b)(1)	Standard: Business associate contracts and other arrangements. A covered entity, in accordance with § 164.306, 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 § 164.314(a) that the business associate will appropriately safeguard the information.	N/A	DNAnexus has a compliant BAA in place with Amazon AWS. No other entities create, receive, maintain, or transmit potential ePHI on DNAnexus' behalf.	
Physical Safeguards				
§164.310(a)(1)	Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	9.1 SECURE AREAS	All DNAnexus production systems and storage are hosted in highly secure Amazon AWS datacenters that have been certified to ISO 27001 standards.	
§164.310(a)(2)	Contingency operations (Addressable). 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.	9.1 SECURE AREAS	Amazon has established geographic redundancy and "availability zones", comprehensive security planning and access controls, and documentation, and has undergone ISO 27001, SSAE-16 and FedRAMP audits of this security.	
§164.310(b)	Standard: Workstation use. 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 electronic protected health information.	7.1.3 Acceptable use of assets	All employees are required to log off or lock workstations when unattended, and workstations are configured to lock when idle. By policy and procedure, potential ePHI is never exported from the Production cloud network by DNAnexus personnel, and is never stored, processed, or transmitted on any DNAnexus workstations. User workstations are periodically audited for proper configuration of malicious code protections, and other security configurations.	
§164.310(c)	Standard: Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	9.2 EQUIPMENT SECURITY	DNAnexus workstations are not used for direct access to potential ePHI.	
§164.310(d)(2)(i)	Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	7.1 RESPONSIBILITY FOR ASSETS	By policy and procedure no potential ePHI is removed from the cloud to any DNAnexus workstations or media. All cloud media, used by Amazon AWS, is securely wiped before disposal. Amazon disposal procedures are audited to ISO 27001, SSAE-16 and FedRAMP standards.	

§164.310(d)(2)(ii)	Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	9.2.6 Secure disposal or re-use of equipment	DNAnexus does not physically handle any sensitive information, and so no sanitization is required. Amazon disposal procedures are audited to ISO 27001, SSAE-16 and FedRAMP standards.	
§164.310(d)(2)(iii)	Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	9.2.7 Removal of property 10.7 MEDIA HANDLING	DNAnexus does not physically handle any sensitive information, and so no movement records are required. Amazon media tracking procedures are audited to ISO 27001, SSAE-16 and FedRAMP standards.	
§164.310(d)(2)(iv)	Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	10.5 BACK-UP	All production customer files are stored in S3, which automatically creates two retrievable, exact copies (with verifying hashes), of all data immediately when stored.	
Security Rule - Technical Safeguards				
§164.312(a)(2)(i)	Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.	11.5.2 User identification and authentication	All customer accounts and DNAnexus accounts used for administration are unique to individuals, with passwords given only to those individuals.	Ensure DNAnexus platform accounts are not shared between individuals, and that individuals do not disclose their passwords to anyone.
§164.312(a)(2)(ii)	Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	10.5.1 Information back-up	DNAnexus has appropriate procedures for secure access to customer data during emergencies.	
§164.312(a)(2)(iii)	Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	11.5.5 Session time-out	PHI Customer accounts lock when idle.	
§164.312(a)(2)(iv)	Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.	12.3 Cryptographic Controls	Potential ePHI is stored in Amazon S3 with AES-256 encryption.	
§164.312(b)	Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	15.3.1 Information systems audit controls	Systems and application logs are enabled and time-synched on all production systems, which include logon/logoff and startup/shutdown events. Logs are regularly reviewed. All logs are transferred from the originating system to secure log servers and to long-term storage where they are protected from unauthorized access or modification.	
§164.312(c)(2)	Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	12.2 CORRECT PROCESSING IN APPLICATIONS	DNAnexus client software uses an MD5 hash on each part of file uploads. Amazon S3 storage also computes MD5 hashes, and both DNAnexus clients and S3 verify these hashes.	
§164.312(d)	Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	11.4.2 User authentication for external connections 11.5.2 User identification and authentication	Passwords are required for customer accounts. Only a few DNAnexus production administrators have remote access to the production network, and two-factor authentication is required for all administration.	
§164.312(e)(2)(i)	Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	12.3 CRYPTOGRAPHIC CONTROLS	DNAnexus client software uses an MD5 hash on each part of file uploads. Amazon S3 storage also computes MD5 hashes, and both DNAnexus clients and S3 verify these hashes. Also, uploads, like all other platform access, are transmitted over secure HTTPS/SSL with built-in integrity mechanisms.	
§164.312(e)(2)(ii)	Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	12.3 CRYPTOGRAPHIC CONTROLS	All platform access is through secure HTTPS connections. By policy and procedure, no potential ePHI is exported by DNAnexus from the secure production cloud. No potential ePHI is processed on workstations where it could be inappropriately emailed. No wireless networks are connected to the production network. All non-production networks are isolated from the production network with stateful firewalls. Customer data is encrypted in the DNAnexus platform when stored.	
Security Rule - Organization and Documentation Requirements				
§164.314(a)(2)(i)	Standard: Business associate contracts or other arrangements.	6.2.3 Addressing security in third party agreements	DNAnexus is amenable to signing a BAA with covered entities, and has a BAA in place with Amazon AWS. By policy and according to DNAnexus' Incident Response Plan, any suspected compromise of potential ePHI data is reported to established customer security contacts.	Sign a Business Associate Agreement with DNAnexus, and contract for a PHI Account with clinical features enabled.
§164.314(a)(2)(ii)	Other arrangements.	15.1.1 Identification of applicable legislation	No Business Associates of DNAnexus are government entities. DNAnexus has obtained satisfactory assurance of HIPAA compliance for all services provided by Business Associates.	
§164.314(b)(2)	Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions...	15.1.1 Identification of applicable legislation	DNAnexus does not manage a group health plan.	
§164.316(a)	Standard: Policies and procedures. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart	5.1.1 Information security policy document	DNAnexus has a comprehensive suite of security policies and procedures, certified to ISO 27001 standards.	
§164.316(b)	Standard: Documentation.	5.1.2 Review of the information security policy	By policy and practice, security policies and procedures are never deleted. Policies and procedures are published on a company wiki. Annual Security Awareness training for all employees communicates policies and procedures, and all employees sign written acknowledgement of their responsibilities. All Security Policies are formally reviewed and approved annually.	
Breach Notification Rule				
§164.410(a)	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	13.1.1 Reporting information security events	PHI Customers will be notified of any suspected breaches of their data.	

§164.410(b)	a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.	13.1.1 Reporting information security events	PHI Customers will be notified within 60 days.	
§164.410(c)(1)	The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.	13.1.1 Reporting information security events	PHI Customers will be notified which accounts and/or project may be compromised.	Be able to identify individuals whose data may have been compromised by a breach.
§164.410(c)(2)	A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under § 164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	13.1.1 Reporting information security events	PHI Customers will be provided "A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known", and "A brief description of what [DNAnexus] is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches".	Communicate directly with individuals affected according to 164.404
Privacy Rule				
§164.500-528	Disclosure, Consent, Notice, Access	15.1.4 Data protection and privacy of personal information	As a Business Associate, DNAnexus does not interact directly with individuals whose data is uploaded by DNAnexus customers. DNAnexus does not use uploaded data for any purpose other than to provide the DNAnexus platform services to DNAnexus customer who uploaded it.	Perform disclosures, obtain consent, give notice, provide access according to Privacy Rule requirements.