Our continuing efforts towards HIPAA compliance are briefed below:

Summary of Key Controls over ePHI	
Encryption	All ePHI data whether in transit or at-rest is bound to be encrypted as per our security policy. Log data involving ePHI is also stored under encryption
Limited Access	We have strictly locked down access to ePHI as per our security policy. The access is granted only when needed and on a temporary basis.
Logging & Monitoring	All interactions (Access/Alteration/Deletion) with ePHI are logged appropriately and are made subject to periodic reviews.
Backups	All customer data is backed up real-time to multiple regions to ensure availability of the same in case of any unforeseen events.

Administrative Safeguards (see 164.308)	
Standard	**Controls in Place**
Risk Analysis (Required)	The risk management program in place involves analyzing all technical and non-technical threats and materializing risks associated with company's assets.
Risk Management (Required)	A formal risk management program is in place as per our security policy that requires security officers to perform continuous risk assessment and monitoring for already identified risks.
Sanction Policy (Required)	A formal sanction policy is in place which is appropriately communicated to employees and they are required to strictly adhere to internal policies are required to avoid sanctions.
Information System Activity Review (Required)	Periodic reviews are in place to identify suspicious activities.
Assigned Security Responsibility (Req)	We have a dedicated security officer who is only responsibility is to ensure that PlatoForms always remains HIPAA compliant.
Authorization and/or Supervision (A	All access logs are reviewed periodically as part of supervisory measure.
Workforce Clearance Procedure (A)	All employee's access is reviewed and approved by independent individuals before the same are actually granted to employees.
Termination Procedures (A)	Termination procedures are in place ensure that access to systems in cut-off effectively and efficiently.
Isolating Health care Clearinghouse Function (Req)	Not Applicable
Access Authorization (A)	As per our access management policy, a formal access request form is required to gain access to systems considering need-to-know basis.

Access Establishment and Modification (A)	All access related activities are performed by an independent resource and similarly are reviewed by security officer on a periodic basis.
Security Reminders (A)	All members of PlatoForms effectively receive the security updates on a timely basis.
Protection from Malicious Software (A)	All endpoints are protected through end-point protection software which are required to be installed as per our security policy.
Log-in Monitoring (A)	All successful and unsuccessful logins are logged for security officer's review.
Password Management (A)	We have policy on creating and managing passwords internally.
Response and Reporting (Req)	A formal incident response plan is in place to guide the internal teams over identifying, investigating, reporting, monitoring and closing incidents.
Data Backup Plan (Req)	A formal data backup schedule is in place which is in-line with the disaster recovery policy of the company. All backups have the duplicated cross region copy. All backups are encrypted.
Disaster Recovery Plan (Req)	A formally approved disaster recovery plan is in place.
Emergency Mode Operation Plan (Req)	Emergency procedures are made part of our business continuity and disaster recovery plan.
Testing and Revision Procedure (A)	As per our policy, we are required to carry out periodic testing of backups and a yearly full-scale test.
Applications and Data Criticality Analysis (A)	All critical resources and systems are identified as part of our business continuity plan.
Evaluation (Req)	As per our policy, we conduct annual or more frequent vulnerability scans in case of any significant changes to application and supporting systems.
Written Contract or Other Arrangement (Req)	All our business associates are HIPAA compliant and formal BAA are in place.

Physical Safeguards (see 164.310)

Standard	**Controls in Place**
Contingency Operations (A)	An approved Business Continuity Plan is in place to guide employees in case of any unforeseen event.
Facility Security Plan (A)	Our outsourced data center is HIPAA compliant and BAA is signed.
Access Control and Validation Procedures (A)	Access to office facilities is strictly controlled. Any access to our infrastructure must via our VPN and the access actives are logged and monitored.
Maintenance Records (A)	All repair and maintenance agreements are appropriately documented.
Workstation Use (Req)	We have an acceptable use policy in place that governs the use of official systems by employees.
Workstation Security (Req)	Workstation use is strictly controlled though security policy and multiple controls are in place to avoid unnecessary access to them.
Device and Media (Req)	We strictly prohibit the use of external media.

Data Backup and Storage (A)	Real time data backups are taken and stored on geographically dispersed locations.
Technical Safeguards (see 164.312)	
Standard	**Controls in Place**
Unique User Identification (Req)	All information systems and company assets are allocated unique identifiers.
Emergency Access Procedure (Req)	Emergency procedures are made part of our business continuity and disaster recovery plan.
Automatic Logoff (A)	As per security policy, systems are configured to log-off sessions after fixed internal of no-activity.
Encryption and Decryption (A)	A cryptography policy is in place that governs the use and management of encryption keys.
Audit Controls (Req)	Periodic audits are carried out to provide an independent opinion on the implemented controls.
Mechanism to Authenticate Electronic Protected (A)	All interactions with ePHI are logged to maintain the integrity of ePHI.
Person or Entity Authentication (Req)	No external access to ePHI is allowed apart from clients. A validation of clients is performed via certificates.
Organizational Requirements (see 164.314)	
Standard	**Controls in Place**
Business Associate Contracts (Req)	All subscribing clients are required to sign BAA as part of HIPAA compliance.
Other Arrangement s (Req)	A separate policy is in place to govern third-party relationships.
Policies and Procedures and Documentation Requirements (see 164.316)	
Standard	**Controls in Place**
Policies and Procedure s (Req)	Formally approved information security policy & procedures are in place.
Time Limit (Req)	ePHI is retained as per Business Associate Agreements in place or for 6 years whichever is higher.
Availability (Req)	All employees are required to adhere to the internal policies and are required to sign-off the acknowledgement accordingly.
Updates (Req)	All internal policies and procedures are reviewed and updated at least annually.