ACHIEVING HIPAA COMPLIANCE WITH POSTGRES PLUS CLOUD DATABASE

TABLE OF CONTENTS

INTRODUCTION

The health care industry is in the midst of a massive transformation aimed at improving patient care and reducing costs. In the U.S., the Affordable Care Act, in concert with regulations such as HIPAA and HITECH, are accelerating the transition to automated processes. Over 80 countries and unions across Europe, Asia, Africa and North America have adopted data privacy and protection laws similar to those in the U.S. However, the information that drives these processes – patient records, clinical test results, medical images, claims data – is highly sensitive. Healthcare and life science stakeholders, therefore, must automate internal and cross-organization workflows while maintaining patient privacy and protecting intellectual property.

HEALTH CARE DATA AT RISK

RESEARCH REVEALS THAT DATA BREACHES COST THE HEALTH CARE INDUSTRY ABOUT $5.6B/YR[1]. ANOTHER STUDY PREDICTS "THE HEALTHCARE INDUSTRY, BY FAR, WILL BE THE MOST SUSCEPTIBLE TO PUBLICLY DISCLOSED AND WIDELY SCRUTINIZED DATA BREACHES"[2].

The HIPAA Final Omnibus Rule, published in January, 2013, mandates that any person or organization which "creates, receives, maintains or transmits" electronic protected health information (PHI) must comply with the HIPAA Security Rule. From a computing perspective, the Final Omnibus Rule effectively requires cloud service providers to share legal responsibility for the privacy of electronically-transmitted PHI.

In the presence of broad health care privacy statutes, organizations are challenged to leverage the economic and scaling benefits of cloud computing while complying with multi-level privacy requirements. EnterpriseDB's Postgres Plus Cloud Database (PPCD), in combination with popular cloud platforms such as Amazon Web Services (AWS), offers a secure, scalable database foundation for a wide range of health care applications.

This paper explores PPCD's advanced security and auditing features. Our goal is to clarify cloud data management and auditing requirements in the context of HIPAA, and discuss how PPCD meets those requirements when deployed on an AWS infrastructure.

FUNDAMENTALS OF HIPAA AND HITECH

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996. Along with increasing the use of electronic medical records, the law included provisions to protect the security and privacy of Protected Health Information (PHI). PHI includes a wide set of personally identifiable health- and health-related data, from insurance and billing information, to diagnosis data, clinical care data, and lab results such as images and test results.

HIPAA was expanded by the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009. HIPAA and HITECH establish a set of federal standards intended to protect the security and privacy of PHI, and impose requirements related to the use and disclosure of PHI, appropriate safeguards to protect PHI, individual rights, and administrative responsibilities. For the purposes of this paper, we'll refer to HIPAA and HITECH collectively as "HIPAA".

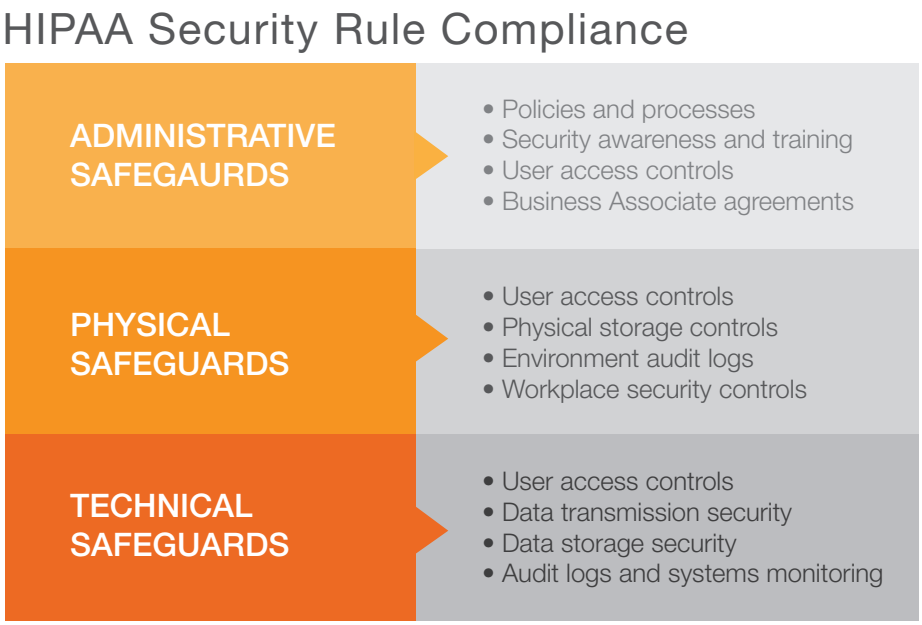
Among its extensive regulatory provisions, HIPAA defines two primary stakeholders:

- Covered Entities – including hospitals, medical services providers, employer sponsored health plans, research facilities and insurance companies
- Business Associates – a person or entity performing activities on behalf of, or providing certain services to, a covered entity while not employed by the covered entity.

The HIPAA Final Omnibus Rule clarifies that any company maintaining PHI on behalf of a covered entity is considered a business associate. Cloud service providers such as AWS are considered HIPAA business associates. Thus, AWS must enter into a business associate agreement with any covered entity on behalf of which AWS stores and transmits PHI.

HIPAA-COMPLIANT DATA MANAGEMENT IN THE CLOUD

To safeguard PHI adequately, organizations must provide a range of operational, technical and environmental controls. Organizations must create compliant business processes; database systems must provide security and auditability; and cloud service providers must deliver secure, controllable execution environments.



As part of its HIPAA business associate agreement, Amazon defines a two-part "shared responsibility model" for implementing secure, compliant cloud environments:

- Security measures that AWS implements and operates – "security of the cloud".
- Security measures that a covered entity implements and operates that relate to content and applications that use AWS services – "security in the cloud".

Health care organizations that have business associate agreements with AWS use the cloud services available in specially-designated HIPAA accounts, ensuring that those services are aligned with HIPAA's security rules (i.e., by supporting the guidelines defined in NIST 800-66). More information about AWS HIPAA compliance is available here.

POSTGRES PLUS CLOUD DATABASE

While AWS provides a HIPAA-compliant cloud platform, health care applications also require a database management foundation for processing transactions, storing structured and unstructured information, and supporting a variety of reporting/analytical requirements. To safeguard PHI adequately, the database manager must complement the capabilities of the platform (AWS, in this case) with a comprehensive suite of security and auditing features.

PPCD is an enterprise class database solution that powers some of the world's most demanding applications. PPCD includes a rich set of database features, elastically scalable performance and built-in high availability – all accessible from an integrated management dashboard.

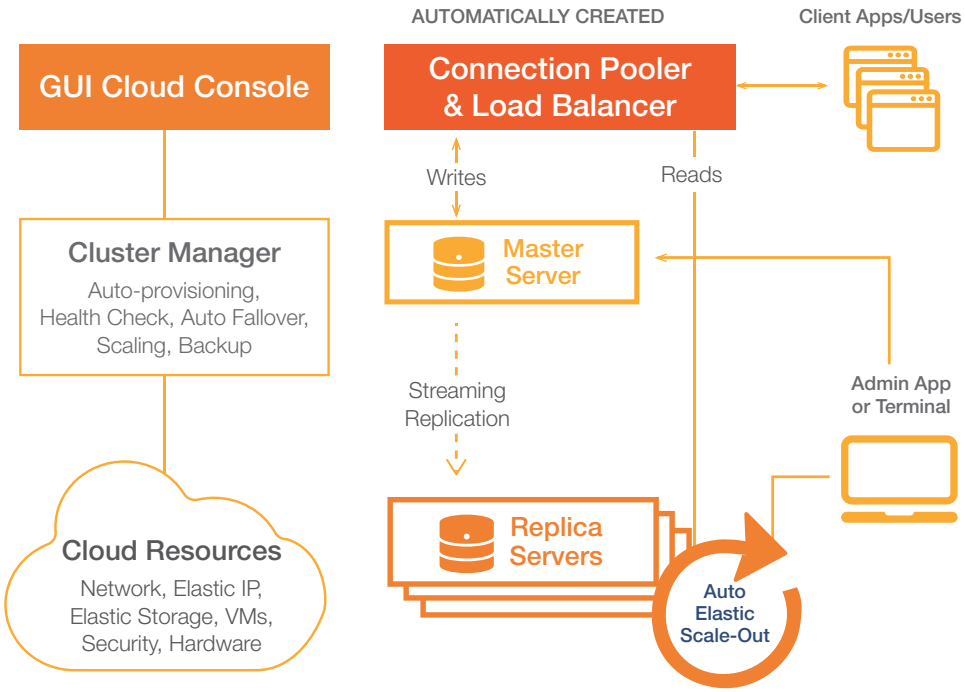
PPCD deploys on AWS EC2 to deliver a secure, compliant data management foundation for a wide range of health care applications. EC2 provides a secure cloud operating environment within which PPCD provides additional PHI security, transaction processing, auditing and database fault tolerance.

Among PPCD's many enterprise features that relate to security-sensitive health care applications include:

PRIVATE INSTANCES WITH CLOSED PORTS	All PPCD databases are deployed using private AWS instances.
AT-REST DATA ENCRYPTION	PPCD uses AES 512 bit cryptography to protect stored data. AES is among the strongest ciphers available in modern computing, and is the cipher standard recommended by NIST.
IN-TRANSIT DATA ENCRYPTION	PPCD generates SSL certificates for every database. Client-side certificates can be generated based on the database certificates and used in client applications.

PASSWORD STORAGE ENCRYPTION	By default, database user passwords are stored as MD5 hashes, so administrators cannot determine user passwords. If MD5 encryption is used for client authentication, the unencrypted password is never present on the server.
CLIENT-SIDE ENCRYPTION	For applications that process highly sensitive data requiring an extra level of security, data can be encrypted and decrypted by the client. Thus, unencrypted data never appears in the database.
ROW-LEVEL SECURITY	Allows an application to authenticate users and set the context for which rows in the database become visible to specific user sessions.
SQL INJECTION PROTECTION	Screens incoming queries for common SQL injection profiles. In addition, PPCD can be configured to accept known queries and reject unfamiliar data request patterns.
DATABASE AUDITING	Allows security administrators and auditors to track and analyze a variety of activities including database access, usage, creation, change and deletion. Audit reports can be viewed using PPCD's DBA Management Server.

PPCD runs as a database cluster on private AWS instances, ensuring that all PHI remains under complete control at all times. The master database, all replica instances, and Amazon storage for the database are managed resources of the AWS HIPAA account.



Each database cluster includes a load balancer,which receives incoming requests from applications and distributes read requests across all read-only replicas within the cluster (unless there are no replicas, in which case the master handles all requests). Write requests are passed directly to the master database.

Applications connect to PPCD databases though defined ports using chosen encryption options. All IDE and development tools can connect to the database by using the address and port information provided when the cluster was created. A Logical Volume Manager (LVM) aggregates storage for the cluster, allowing transparent scaling of cloud storage without adversely affecting running databases.

In addition to the security and compliance-related capabilities described above, PPCD provides other powerful features that are often critical to health care applications, including:

- ACID compliance – PPCD is a 100% ACID compliant relational DBMS. Its proven, high performance transaction engine powers many of the world's most advanced mission-critical applications.

- Rich data types – Postgres is renowned for supporting a wide variety of structured, semi-structured and unstructured data. Unlike NoSQL datastores, which operate under eventual consistency semantics, all PPCD data is managed transactionally to ensure it is consistent and accurate at all times. Using PPCD, applications leverage the simplicity and power of a single, flexible data management infrastructure.

- Integration – PPCD's foreign data wrappers (FDW) provide a simple and powerful way to interoperate with external data sources. Health care application developers and DBAs can use FDWs to easily aggregate data from companion systems to create a single, integrated database. FDWs save significant time and costs for applications requiring database interoperability.

- Portability – Postgres is available from multiple vendors – on-premise, in virtualized environments and in the cloud. Freedom of choice eliminates vendor lock-in and stimulates a vibrant, competitive market for Postgres products and services.

- Compatibility – PPCD delivers comprehensive Oracle® compatibility, allowing health care organizations to leverage their Oracle database investments while transitioning to the cloud. Oracle DBAs and application developers can use their existing skills, tools and practices to implement new systems using PPCD. In addition, EnterpriseDB offers Oracle Migration Services to assist organizations to migrate existing Oracle applications to PPCD.

SUMMARY

HIPAA's privacy protections require sensitive health care data to be stored and transmitted in a highly secure manner. PHI must be encrypted in transit and at rest, and stakeholders must provide comprehensive governance and auditing in every aspect of PHI data management.

To leverage the financial and scaling benefits of cloud computing, health care organizations require a HIPAA-compliant cloud data management solution. Deployed on AWS private instances within an AWS HIPAA account, EnterpriseDB's Postgres Plus Cloud Database combines a powerful suite of security and auditing features with those available from EC2. PPCD enables health care organizations to build and deliver secure, compliant database applications on AWS. Combined with sound compliance practices and governance, PPCD allows organizations to confidently leverage the benefits of the AWS cloud environment.

Beyond compliance, PPCD also provides proven enterprise-grade capabilities needed for superior performance, effortless scaling and high availability. Organizations can deploy applications on PPCD knowing that their chosen database is the foundation of many of the world's most web applications.

For further information about EnterpriseDB and PPCD, please visit us at http://www.enterprisedb.com/Cloud or email sales@enterprisedb.com.

COVERED ENTITY APP

- User access controls
- Application audit logs
- Compliance monitoring

PPCD DATABASE

- User access controls
- Data encryption in transit
- Data encryption at rest
- Database audit logs

AWS INSTANCE

- User access controls
- Physical location controls
- Platform audit logs
- Workplace security controls

FOOTNOTES

1. Fourth Annual Benchmark Study on Patient Privacy & Data Security – Ponemon Institute LLC
2. *2014 Data Breach Industry Forecast* – Experian Information Solutions, Inc.