<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security, Compliance and Digital Transformation in Healthcare</td>
</tr>
<tr>
<td>Cloud Essentials</td>
</tr>
<tr>
<td>Healthcare Digital Transformation</td>
</tr>
<tr>
<td>Cloud Provider Security Attributes</td>
</tr>
<tr>
<td>Deeper Dive</td>
</tr>
<tr>
<td>Case Study</td>
</tr>
<tr>
<td>Q &amp; A</td>
</tr>
</tbody>
</table>
Definitions: Service Models

- **Infrastructure as a service (IaaS)**
  - Self-provision for processing, storage and networks
  - Ability to deploy arbitrary software
  - Consumer does not manage underlying cloud infrastructure
  - Examples: Amazon Web Services, Microsoft Azure, Google Cloud Platform

- **Platform as a service (PaaS)**
  - Deploy applications created using languages and tools supported by the cloud service provider
  - Examples: Force.com, Heroku, Google App Engine, Elastic Beanstalk (AWS)

- **Software as a service (SaaS)**
  - Consumers simply use the software
  - Examples: Office 365, Gmail.

- **Communications as a service (CaS)**
  - Examples: Skype

- **Data Storage as a service (DSaaS)**
  - Examples: Dropbox, Box, Google Drive, Microsoft One Drive
Definitions: Cloud deployment models

- **Public cloud**
  - Services are available to *any cloud customer*, but resources are controlled by the cloud service provider (CSP)
  - May be owned, managed and operated by business, government and academic organization
  - Subject to jurisdictional regulations
  - Examples: Amazon Web Services, Microsoft Azure, Google Cloud Platform

- **Private cloud**
  - Services are available only to *single cloud customer*, but resources are controlled by CSP
  - May be owned, managed and operated by business, government and academic organization
  - Examples: Amazon Web Services, IBM private cloud services, Azure Pack, OpenStack

- **Hybrid cloud**
  - Interactions between two different deployments needed but remained linked
Clarifications: What’s not cloud

• Out sourced IT or remote data centers
• Virtual machine hosting
• Remote login or desktop
• Web based applications or sites
• Client-server computing or distributed computing
On premises VS. Cloud Computing

On-Premises:
• CAPEX Funding
• Compute resources managed by organization
• Organization remains full control over data and applications

Cloud computing:
• Typically Opex funding (Utility model with lower total cost of ownership)
• Compute resources managed by provider
• Control and access to data should not be compromised
Digital Transformation is Business + Technology

• Digital Transformation is Digital Business
• Digital Transformation is Digital Technology
  • Technology Modernization embracing Agile architecture that is flexible, stable, reliable – architecture across on-prem, co-lo, public cloud(s) – hybrid is the end state
  • Data Driven – Machine/Deep Learning, AI, Bots, Structure and Un-Structured
  • Security, Privacy, and Regulatory Compliance must be fully supported
Scenarios for Healthcare
Digital Transformation Pillars in Healthcare

Digital Transformation Pillars

- ENGAGE MEMBERS
  - More Efficient Access
  - More Efficient Engagement
  - More Continuous Engagement

- EMPOWER CARE TEAMS, UTILIZATION
  - Virtual Care
  - Care Team Collaboration
  - Care Coordination

- OPTIMIZE CLINICAL & OPERATIONAL EFFECTIVENESS
  - Quality Improvement
  - Population Health
  - Operational & Financial Efficiency

- TRANSFORM THE CARE CONTINUUM
  - Remote Monitoring/Rural Health
  - Precision Health
  - Managing Devices & Facilities

Trusted Technology – enabling Security, Privacy, & Regulatory Compliance
Why? - “New Designs” to enable the Triple Aim

- At Microsoft Health and Life Sciences, we believe in the Institute for Health Improvement’s (IHI) Triple Aim framework (http://www.ihi.org/offerings/Initiatives/TripleAim) to optimizing health system performance.

- IHI states that New designs must be developed to simultaneously pursue the three dimensions of healthcare transformation called the “Triple Aim”.
  1. Improving the patient experience of care (including quality and satisfaction)
  2. Improving the health of populations
  3. Reducing the per capita cost of health care
  4. Improving the work life of clinicians and staff

We suggest defining digital transformation in health as "technology enabled care, health promotion and disease prevention that advances the triple aim in a mobile-first and trusted, cloud-first world.

"The “Triple Aim” is Microsoft’s health industry gold standard – “Dr. Dennis Schmuland, Microsoft Chief Health Strategist”
Foundational Components of Digital Transformation

- Not mutually exclusive
- Not optional
- Not negotiable

Required across the extended enterprise
A digital business environment characterized by volatility and disruption will lead to industry fluidity. CIOs must understand that business transformation is called for in this high-risk environment, the bedrock of which will be the technology foundation supporting digital business. - Gartner Research, December 2015

...Digital transformation maturity and intensity consists of the vision to shape a new future, governance and engagement to steer the course and IT/business relationships to implement technology-based change...On average, Digital Conservatives and Digirati are 9% to 26% more profitable than their average industry competitors... - MIT Sloan November 2012
Big data allows companies to make meaningful, strategic adjustments that minimize costs and maximize results....A digital transformation isn’t complete unless a business adopts big data. - Forbes
December 2015

...data-driven methods enhance revenue generation and enable cost reduction, as well as accelerate process efficiencies and quality improvements...- Forbes Insights Survey
May 2016
While exploring the potential of new, data-driven business models, companies need to tackle how to manage security and privacy more effectively...

- Enterprise Innovation
  October 2016

Companies need to rethink their approach to security... The approach we recommend is really founded on the fact that security is part of the entire life cycle. It should be catered to at the start of the digital transformation... Raymond Teo
  SVP NTT Security’s APAC Field Operations

Survey
Top technologies with greatest impact:
1. Cloud computing
2. Analytics
3. Mobility
4. Security
Trusted Cloud Principles
Commitment to trusted principles

<table>
<thead>
<tr>
<th>Security</th>
<th>Privacy &amp; Control</th>
<th>Compliance</th>
<th>Transparency</th>
</tr>
</thead>
<tbody>
<tr>
<td>The confidentiality, integrity, and availability of your data is protected.</td>
<td>No one is able to use your data in a way that you do not approve.</td>
<td>Your content is stored and managed in compliance with applicable laws, regulations and standards.</td>
<td>You have visibility into how your data is being handled and used.</td>
</tr>
</tbody>
</table>
Cloud Provider Security
Covering Physical, Technical, and Administrative Safeguards – Just like a Covered Entity

Physical Security
• 24-hour monitoring of data centers; Multi-factor authentication, including biometric scanning for data center access.
• Internal data center network is segregated from the external network.
• Role separation renders location of specific customer data unintelligible to the personnel that have physical access.

Logical Security
• Defense in depth – data, user, app, host, network, network perimeter, facility with disaster recovery and data geo-redundancy/failover
• Lock box processes for strictly supervised escalation process limiting human access to your data.
• Servers run only processes on whitelist, minimizing risk from malicious code.
• Dedicated threat management proactively anticipate, prevent, and mitigate malicious access.
• Port scanning, perimeter vulnerability scanning, and intrusion detection prevent or detect any malicious access.

Data Security
• Drives encrypt data at rest
• All in transit data encrypted between you and cloud data centers with SSL, PFS (2048 bit), TLS, Ipsec
• Threat management, security monitoring, and file/data integrity prevents or detects any tampering of data.

Admin and user controls
• RMS, MFA, Message Encryption, DLP
Cloud Provider Privacy

Customer ownership of data

- You are the owner of the data
- It’s your data, so if you ever choose to leave the service, you can take your data with you;
- Your data is not mined or sold for advertising or analytics purposes

Transparency about your data

- We only use your data for purposes consistent with providing you services
- If a government approaches for access to customer data, the inquiry is redirected to you, the customer, whenever possible and will challenge in court any invalid legal demand that prohibits disclosure of a government request for customer data.

Privacy controls for customer

- Privacy controls allow you to configure who in your organization has access and what they can access.
- Design elements prevent mingling of your data with that of other organizations.
Cloud Provider Compliance (Musts)

**HIPAA**
- Prevent inappropriate use and disclosure of individual health information.
- Administrative, Technical and Physical Safeguards
- BAA

**FedRAMP**
- Accelerate adoption of secure cloud solutions
- Increase confidence in security of cloud solutions
- Increase automation for near real-time data for continuous monitoring
- Government Data isolation

**HITRUST**
- A certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management.
- HITRUST CSF rationalizes healthcare-relevant regulations and standards into a single overarching security framework

**ISO 27001/27018, NIST, PCI, GDPR**
Health Care Providers’ Due Diligence

Risk Assessments
- Verify safeguards are in place
- Know full scope of impact if there’s a security incident
- Compare different cloud service providers

Data Security Documents
- Agreements/addendums set out expected security controls
- Breach response expectations
- “Audits” on routine basis
- Insurance requirements

Communicate
- Business units need to know what to expect beforehand
- Timeframes vary based on service provider responsiveness and scope of services
Microsoft Cloud
Largest Compliance of any cloud provider

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>UNITED STATES</th>
<th>REGIONAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27018</td>
<td>FedRAMP JAB P-ATO</td>
<td>Argentine Data Protection Act</td>
</tr>
<tr>
<td>SOC 1 Type 2</td>
<td>HIPAA / HITECH</td>
<td>European Union Model Clauses</td>
</tr>
<tr>
<td>SOC 2 Type 2</td>
<td>FIPS 140-2</td>
<td>United Kingdom G-Cloud</td>
</tr>
<tr>
<td>SOC 3</td>
<td>21 CFR Part 11</td>
<td>Canadian Privacy Laws</td>
</tr>
<tr>
<td>PCI DSS - Level 1</td>
<td>FERPA</td>
<td></td>
</tr>
<tr>
<td>ISO 27018</td>
<td>DISA Level 2 (DIACAP)</td>
<td></td>
</tr>
<tr>
<td>CSA security</td>
<td>ITAR readyl</td>
<td></td>
</tr>
<tr>
<td>Alliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISA/IEC 27017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Matrix v3.0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPAA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shared Assessments</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- FedRAMP
- HIPAA / HITECH
- FIPS
- 21 CFR Part 11
- FERPA
- DISA Level 2 (DIACAP)
- ITAR
- CJS
- IRS 1075
- ITAR-ready
- Section 508
- VPATs
- FISMA
- NIST 800-171
- Centers for Medicare & Medicaid Services
- GxP
- DIACAP
- MARS-E
- GxP
- DIACAP
- China Multi Layer Protection Scheme
- Japan My Number Act
- Argentina Data Protection Act 25.326
- Chinese GB 18030
- China TRUCS
- Singapore MTCS Level 3
- New Zealand GCIO
- Japan Financial Services
- ENISA IAF
- Cloud Security Mark Gold
- Spain ENS
- FACT
- EU-US Privacy Shield
- NZCC Framework
DEEPER DIVE
HEALTH CARE DATA IN THE CLOUD
Cloud Responsibility Matrix

<table>
<thead>
<tr>
<th>Security Governance, Risk &amp; Compliance (GRC)</th>
<th>Infrastructure as a Service (IaaS)</th>
<th>Platform as a Service (PaaS)</th>
<th>Software as a Service (SaaS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>Enterprise Responsibility</td>
<td>Shared Responsibility</td>
<td>Cloud Provider Responsibility</td>
</tr>
<tr>
<td>Application Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platform Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security Principles:
- Secure by default
- Least Privilege
- Role separation
- Mitigation of credential theft attacks
- Known good components
Healthcare Data – Cloud Secure Access and Storage

**OLTP Applications/Data**
- Business Process
- Data Genesis
- Short Lived Queries (Transactions)
- Speed and Integrity
- Usually Schema Bound
- Operating Dataset
- Riddled with PHI/PII
- Strict Access Control/Auditing

**OLAP Applications/Data**
- Analytics/Data Mining
- Decision Making
- Complex Queries (Aggregate)
- Longer running/More Compute
- Little Schema Integrity
- Large Datasets
- De-Identified (Correlation Ids)
- Possibly Less Restrictive Access
<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>PHI/PII</th>
<th>De-Identified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption at Rest</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Encryption in Transit</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Key Management &amp; Ownership</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Access Logging/Auditing</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Id Proofing/Authentication</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Multi-Factor Authentication</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Secure VPN/Direct Connection</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Limited-Life Span Spoof Proof Access Token</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>
Healthcare Data – Cloud Secure Access and Storage
Healthcare Data - Data Security and Encryption

Encrypted
- At-rest: all information storage objects, containers and types that exist statically on physical media
- In-Transit: data transferred between components, locations or programs. Over a network, service bus, cloud->on-premise, etc...
- User controlled Keys (BYOK/HYOK) stored in secure container (HSM) with RBAC
- Dual layer key protection: Data encrypted with encrypting key which is encrypted with a master key
- Key rotation: Rotate master key on shorter schedule to protect encrypting key, rotate encrypting key less frequently.
- Use OS level encryption for VMs (DM_Crypt, bitlocker, etc.)
- Enforce TLS, SSL, VPN (IPSEC) with Firewall, Services and vnet access

Access Control
- Enforce Multi-Factor Authentication
- Read only access to decrypt master key controlled by RBAC
- RBAC to storage objects
- Application/Service/Function level RBAC
- OAuth 2.0 PKI Signed JWT tokens for Authorization (claims, RBAC, lifespan and spoofing)
Healthcare Data - De-Identification

Compliance
- HIPPA Expert Determination/Safe Harbor Attributes
- Low/High Risk Attributes

Correlation Id
- Enable action on insights gained in analytics
- Non-Deterministic/Encrypted Specialized Key
- Processed in secure cloud or on-prem
USE CASE
Summary: Cloud benefits

• Easy to use
  – Management console access
  – Well-documented resources

• Cost-effective
  – Pay for use of resources;
  – Availability of reserved resources at deep discount

• Reliable, Scalable and high performance
  – Auto scaling; elastic load balancing
  – Access to compute and storage needs on demand

• Flexible
  – Choice of your Operating system, programming language, application platform and database

• Security and compliance
  – End-to-end secured and hardened infrastructure
Cloud challenges

- Choice of IaaS, PaaS and SaaS
  - Business strategy
- Lack of executive support
  - Un-quantified benefits make prioritization difficult
  - Align proposal with business strategy
- Control mechanisms shift
  - How to ensure compliance with business practices and objectives?
  - Empower IT org to become Center of Excellence for cloud
- Flexibility (Vendor lock-in)
  - Data portability is essential
  - Understand data ownership and retention policies
- Security and compliance
  - Regulatory compliance and visibility is essential
  - Implicit compliance needs to be engineered
- Integration
  - Tools and knowledge of systems integration with existing applications
Health care provider challenges

• Processes
  – New, existing or none at all
  – Enterprise buy-in
  – Communication

• Culture clash
  – Business units, service providers, the Enterprise as a whole

• Risk vs. Value
  – Where is “good enough?”
PEOPLE, PROCESS AND TECHNOLOGY
Goals of stakeholders

• Providers, payers, technology companies and life science companies want to
  – Improvise / modernize infrastructure
  – Secure, protect patient data and adhere to compliance
  – Improve data usage across teams
People

• IT Leaders require
  – Control, visibility, cost transparency issues addressed
• IT line managers expect
  – Performance and administration concerns addressed
• Internal and third party auditors require
  – Evidence for implementation of technical and procedural controls
• Business leaders want
  – Quick Proof of concept
  – Cost reduction using automation
• Compliance and legal need
  – Early insight and input
Process (Step 1 of 4)

Discovery

- Overview and understanding of the existing architecture of the applications
- Essential compliance and legal requirements
- Business requirements (cost, scalability)
- Success criteria
- Overall SLA requirements and impact of application
- Team support from customer and provider / integrator
- Vision for desired state Vs. current state
Process (step 2 of 4)

Design

- Application modification
- Test cases to be tested
- Upgrade path / testing scope
- Performance / Usability / Security / Availability
- Failover
- Monitoring tools needed
- Data backup and retention
- Cost calculator for compute, storage and network
- Cost estimation for on-going monitoring, tools and support
- Deployment creation – designing infrastructure as a code
- Licensing requirements from application perspective and how infrastructure can provide support
- Compliance readiness and assessment
Process (step 3 of 4)

Implementation

- Creating cloud account architecture and network topology
- Detailing security architecture for instances
- Setting up instances, operating systems, application technology stack
- Setting up / configuring for data ingestion
- Data backup, recovery, retention and archiving
- Software and tools for monitoring and managing

- Automation
  - VPC setup using cloud formation / resource manager templates
  - Automating instance creation, OS images and keeping them ready for application load
  - Readiness for production including monitoring
Process (step 4 of 4)

Deployment and Go-live

- Repeat the implementation phase using infrastructure as a code concept
- Following tools and repositories may be used for deployment
  - Ansible, Chef and Cloud formation / Resource Manager templates
  - Jenkins and Github
Technologies - How two big cloud providers compare for healthcare – Tough choice

<table>
<thead>
<tr>
<th>Offerings</th>
<th>AWS</th>
<th>Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-scaling</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual machines (temporary and dedicated)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Durable and long term Storage</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security and access - HIPAA, PCI, ISO 27001, FEDRAMP, SSAE-16</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Key management services - Encryption at rest and in motion</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>- Identity and access management</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SLAs, Support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Migrating a medical device manufacturer’s software to cloud
Goals for migration

- Business goals – Cut costs by 15%, create a center of excellence for cloud
- Technology goals – Setup highly available and DR environment
- Compliance goals – Provide automated evidences for compliance
- Migration goals – Complete the migration in 3 weeks and provide for regression testing
Best Practices in Cloud

- Business Associate agreement
- Policies, governance and ownership
- Coverage for Security policy
- Establish cloud center of excellence
- Best practices in implementation
  - Accounts, network and security policy
- Automation
  - Infrastructure as a code
  - Evidence collection
- Choice of offerings
Who owns what?

Customer
- Data
- Application
- Networking services
- Computing services
- Policies, Procedures, Awareness

Cloud service provider
- Internal Network
- Perimeter
- Physical
Obtain Business Associate Agreement

• All good cloud service providers agree to BAA with customer
1. Confidentiality
   1. Encryption at rest
   2. Encryption in motion

2. Integrity
   1. IAM roles
   2. Groups and roles

3. Availability
   1. High availability zones
   2. Disaster recovery and business continuity
Team composition

- Cloud practice director
- Cloud solution architect
- Cloud DevOps engineers

Benefits

- Gain support from executive team
- Low cost experimentation to stay relevant
- Create hybrid organization
Master-sub accounts benefits

• Separate accounts for development and production
• Consolidate billing, but charge back to individual departments made easier
Network setup

- Multiple VPC and gateway
  - Separate development from production
  - Document access to separate network
Multiple security groups

- Isolate rules for access, keys, inbound and outbound connection
- Attach policies as a service
- Attach roles to groups and users
Benefits:

- Reduces human errors
- Improves consistency in adopting security policies.
Benefits:

- Reduces operational overhead
- Improves influence of CIO organization
What can be automated?

Infrastructure as a code

- Data encryption at rest
- Network traffic encryption
- Automated backups
- System monitoring and alerting
- VPC and security groups
- System access controls and logging
- Operating system: maintenance, management and patching
- Logging: Aggregation and archiving
<table>
<thead>
<tr>
<th>Offerings</th>
<th>AWS</th>
<th>Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-scaling</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual machines (temporary and dedicated)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Durable and long term Storage</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security and access - HIPAA, PCI, ISO 27001, FEDRAMP, SSAE-16</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Key management services</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>- Encryption at rest and in motion</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>- Identity and access management</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SLAs, Support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
EVIDENCE FOR AUDITS
Automated backups

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance/Cluster Name:</td>
<td>prod-i db</td>
</tr>
<tr>
<td>Snapshot Type:</td>
<td>automated</td>
</tr>
<tr>
<td>DB Engine Version:</td>
<td>5.5.33</td>
</tr>
<tr>
<td>Master Username:</td>
<td>(blank)</td>
</tr>
<tr>
<td>Zone:</td>
<td>us-east-1d</td>
</tr>
<tr>
<td>Storage Type:</td>
<td>(blank)</td>
</tr>
<tr>
<td>Option Group:</td>
<td>default:mysql-5-5</td>
</tr>
<tr>
<td>KMS Key ID:</td>
<td>31d08e06-17cc-439b-b691-895e053a7aad</td>
</tr>
<tr>
<td>Source Region:</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Encryption at rest

<table>
<thead>
<tr>
<th>Description</th>
<th>Status Checks</th>
<th>Monitoring</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume ID</td>
<td>vol-0a5abcabc42093b34</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td>1024 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Created</td>
<td>March 6, 2017 at 1:11:52 AM UTC-8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>in-use</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attachment Information</td>
<td>i-07a0409fafa6a75fe6b (prod-)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volume type</td>
<td>gp2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product codes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IOPS</td>
<td>3072</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm status</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Snapshot</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability Zone</td>
<td>us-east-1b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted</td>
<td>Encrypted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMS Key ID</td>
<td>c726fa4cc-f5ec-4811-94a5-0291d2408f</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMS Key ARN</td>
<td>arn:aws:kms:us-east-1:9527737433:...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Encryption in motion
System Monitoring and alerting
VPC and Security Groups
System access controls
Logging and audit trails