BYTEGRID®

21 CFR COMPLIANT CLOUD HOSTING

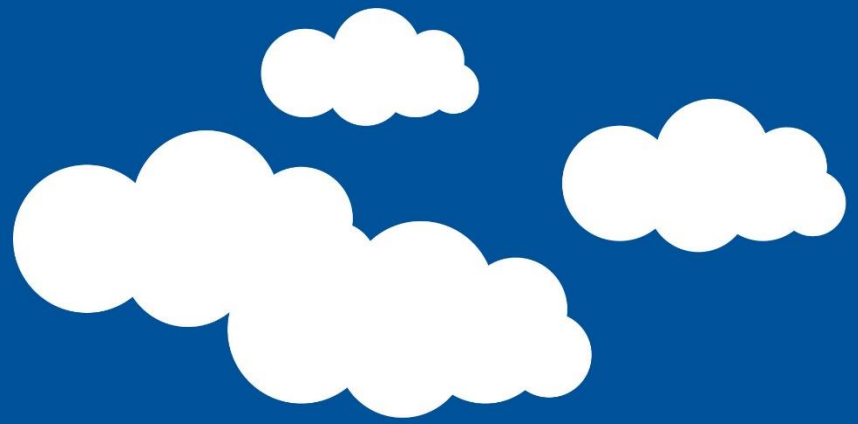
Speaker Bio

Rebecca Santorios is Director of Compliance at ByteGrid. In that role, she is responsible for ensuring compliance to GxP and HIPAA compliance within the ByteGrid organization, and for providing compliance services to ByteGrid's regulated clients. Prior to joining ByteGrid, Rebecca served as a compliance consultant to organizations throughout the GxP vertical, after having held senior compliance positions in medical device and pharmaceutical organizations. Rebecca has a background in biochemical engineering, with additional studies in system engineering, and over 15 years of experience implementing and validating computerized systems in the GxP space. Rebecca is an active member of ISPE and is an ASQ CQE.

Agenda

- Cloud Description and Cloud Models
- Cloud Benefits, Risks, and Challenges for Medical Device Systems
- Regulatory Considerations
- Use Cases
- Questions

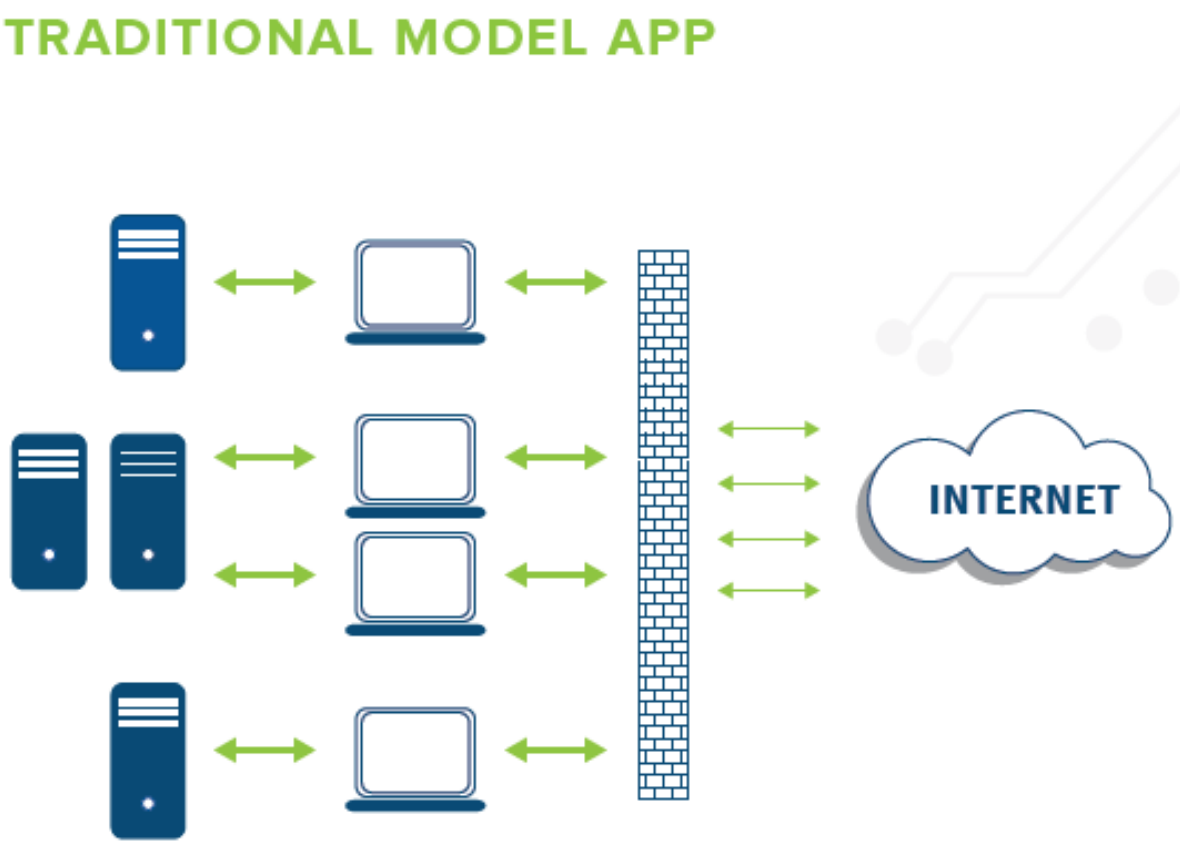
CLOUD DESCRIPTION AND CLOUD MODELS



NIST Definition of the Cloud

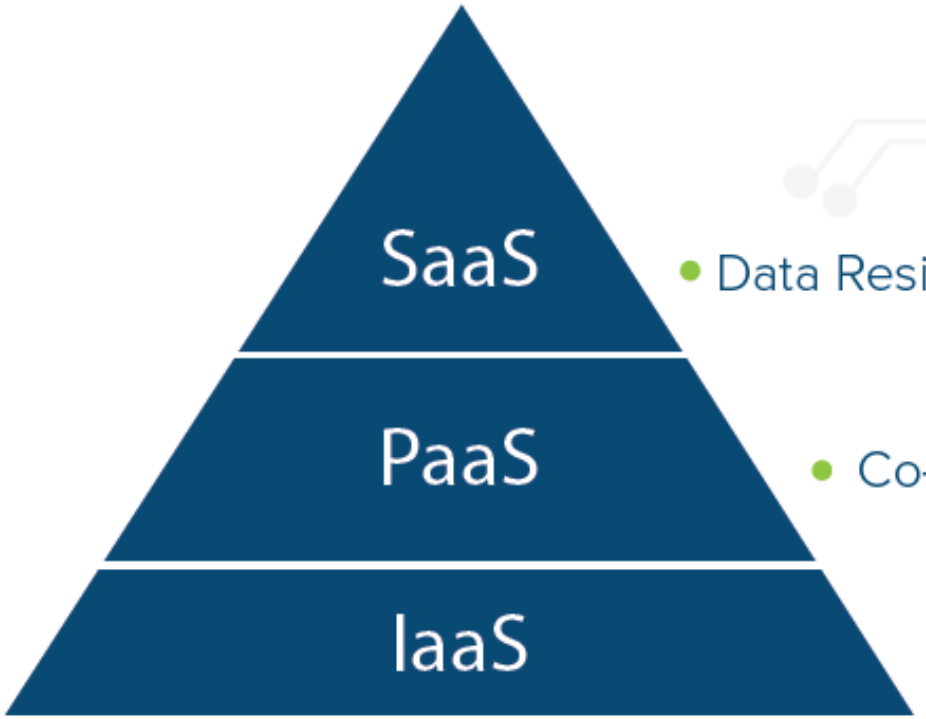
- Essential Characteristics
  - On Demand self-service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured service
- Service Models
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
- Deployment Models
  - Private Cloud
  - Community Cloud
  - Public Cloud
  - Hybrid Cloud

Traditional Model App



- Physical Servers
- Hardware on Site
- QA & Prod Servers IQ'd
- QA used for OQ
- PROD used for PQ
- Client PC's have Client side Application Software
- Contained Behind Corporate Firewall
- Infrastructure Considered 'Low Risk'

Cloud Model



- Data Resides with Cloud Provider
- Co-tenant can impact security
- Many Configuration Points

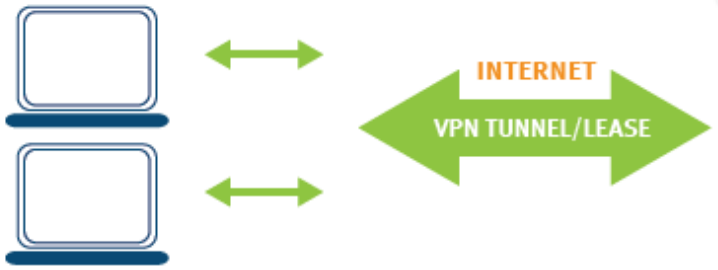
Cloud: In-house vs External

- SAS 70 Type 2, SSAE16, and ISO27001 do not equate to alignment with GxP or 21 CFR Part 11
- While larger companies can afford to procure the infrastructure necessary to build an internal cloud most companies will seek to outsource
- Most regulated companies have already engaged at least one XaaS provider
- Very few SaaS providers have their own datacenters, many IaaS and PaaS providers also lease space
- Vast majority of datacenters hosting regulated data do not have FDA centric controls or qualification in place.

Colocation Model

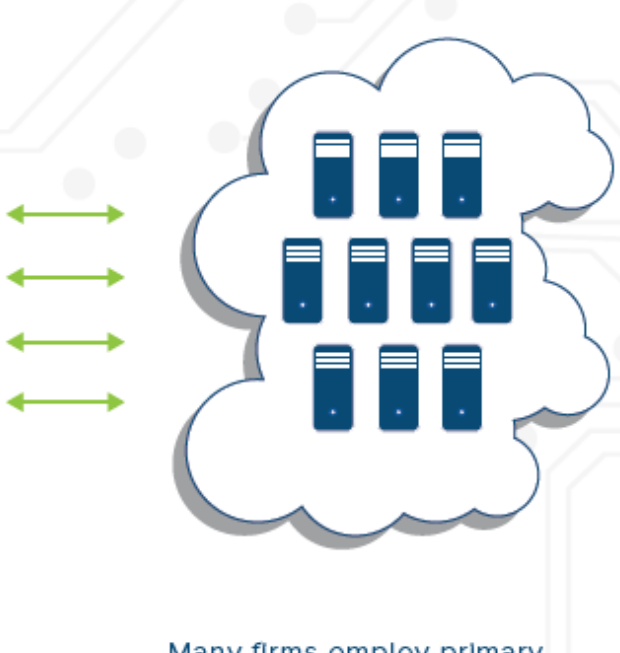
COLOCATION MODEL

- Hw IQ - Regulated entity / Data Center
- Sw IQ - Configured in application
- OQ - On demand/fixed test environment
- PQ - Server power controlled by regulated entity



- Firm 'rents' power, HVAC, Physical Security
- Data travels over VPN
- Properly configured VPN highly secure
- Reg entity owns server hardware
- Data managed internally
- Bandwidth subject to Data Center constraints

INFRASTRUCTURE OFFSITE

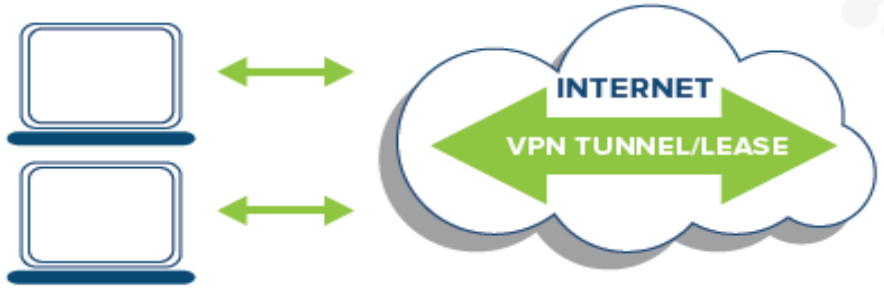


Many firms employ primary and secondary data centers with replication and mirroring

Infrastructure as a Service Model

INFRASTRUCTURE AS A SERVICE MODEL

- Hw IQ - 3rd Party/RE/DC
- Sw IQ - configured in cloud
- OQ - on demand test environment
- PQ - performance needs definition

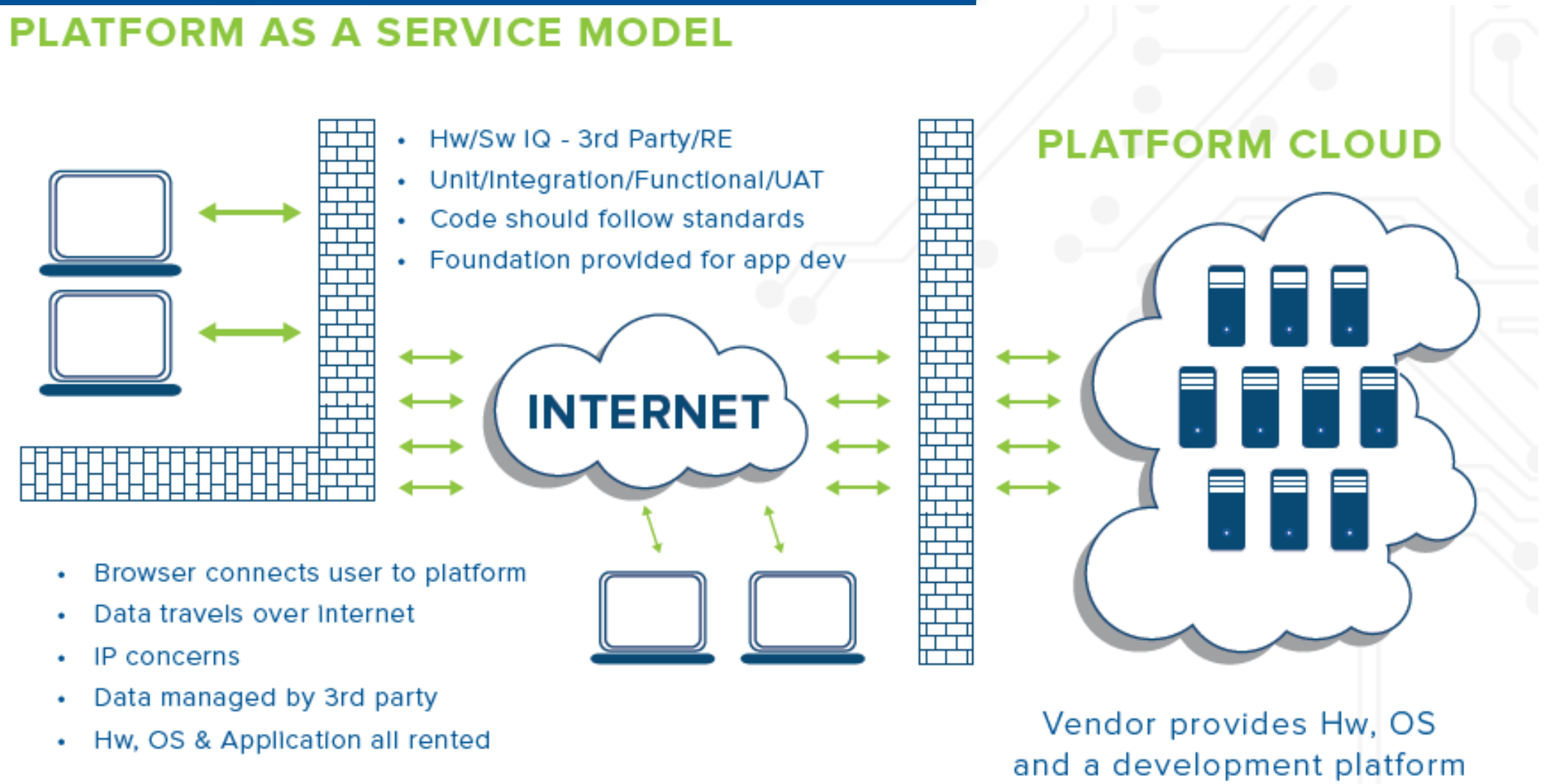


- Firm 'rents' infrastructure
- Data travels over VPN
- Properly configured VPN highly secure
- Reg Enttly controls OS up
- Data managed internally
- Elasticity: pay for what you need

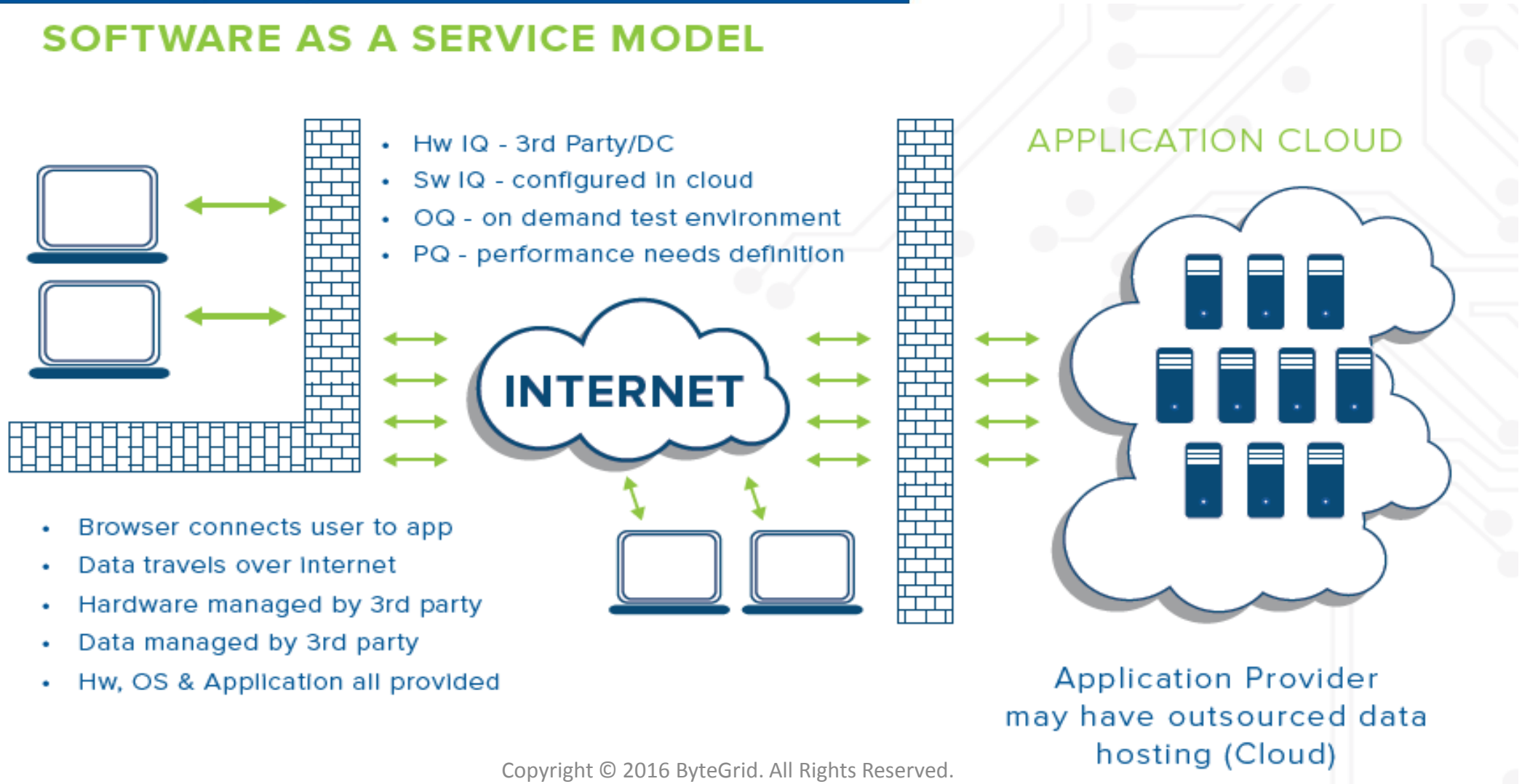
INFRASTRUCTURE CLOUD

Many firms employ primary and secondary data centers with replication and mirroring

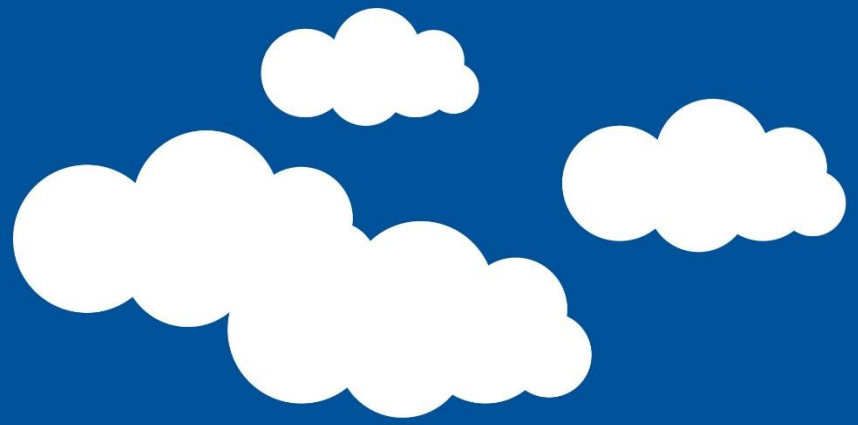
Platform as a Service Model



Software as a Service Model



CLOUD BENEFITS, RISKS, AND CHALLENGES FOR MEDICAL DEVICE SYSTEMS



General Cloud Benefits

- Broad network access
- Resource pooling
- Rapid elasticity
- Le$$ on IT more on R&D
- Focus on core competencies
- Access to economies of scale
- Lower cost to patient

Medical Devices – Drivers for Moving to the Cloud

- Local installations - PC often at the mercy of customer Lab/IT personnel
- Can lead to nefarious customer complaints, time, money, resources and reputation all expended because of antivirus or other 3rd party installation, potential for operation outside validated state
- Some systems can have install bases in the thousands – often on varied versions of the software
- Regulatory challenges related to non-homogenous installed base
- Impossible to accurately assess risk with cross version pollination and 3rd party installs
- Generated data generally lives within customer organization and labs – little or no insight relative to patient demographics

Medical Devices – Benefits of Moving to the Cloud

- Virtualizing the environment can greatly reduce the regulatory burden
- PCs being phased out by OEM no longer a concern, reducing hardware driven ECRs
- Eliminates (or reduces), PC/server cost
- Reduces field service resource drain
- Takes burden away from lab/customer IT to maintain
- Real-time maintenance and use metrics
- Eliminates nefarious installs

Medical Devices – Benefits of Moving to the Cloud

- Homogenous version – easy to update and maintain
- Improves patient & operator safety – keeps ‘approved’ version with ‘cleared’ footprint in place
- Smaller footprint in the lab – more room for more equipment
- Even if a PC is still required (e.g. instrument control), can be less powerful ‘dummy terminal’
- Reduced risk of data integrity violations due to inappropriate system actions (file access, operating system changes, clock changes)

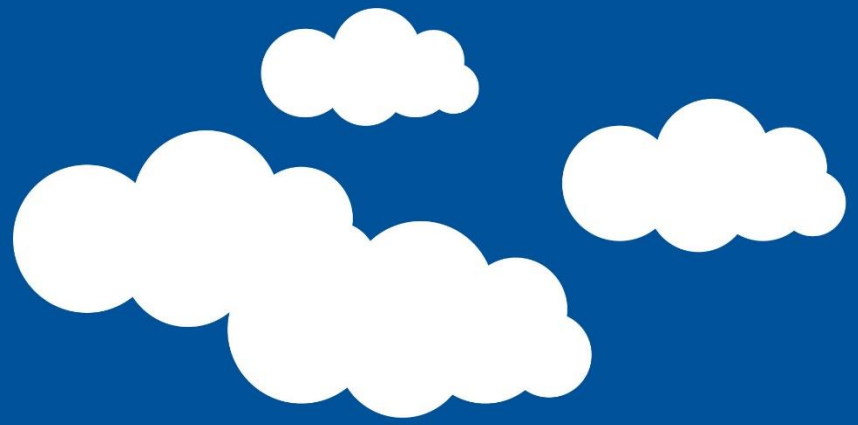
Revenue and Cost Reduction Opportunities

- Reduction on hardware spend
- Reduction of Field Service spend
- Reduction of product complaints
- Decreased opportunity for patient/operator safety issues
- Multiple versions and associated support costs can be phased out
- Real-time kit inventory and replenishment – across installed base
- Big Data
- Data collected across customers can now be analyzed and monetized
- Analytics as a subscription based service
- New market opportunities and customer groups
- Opportunity to bring lab information directly into the hands of medics and patients

Cloud Computing Challenges

- Loss of physical control
- Security models and standards are still emerging
- Vendor failures, notably starts-ups
- Responsibilities not always understood
- Isolation/security between virtual machines
- Guest to host communication internet based
- Vulnerability of browsers
- Data privacy implications
- Availability concerns
- Implications for e-discovery
- Customer support practices are evolving

REGULATORY CONSIDERATIONS



Regulatory Implications for Medical Devices

Depending on type of system, there can be major 21 CFR 820 impact					
§ 820.5	Quality System Documentation	§ 820.70	Manufacturing records, ECO/ECR	§ 820.160	Distribution records
§ 820.22	Audit records	§ 820.72.	Calibration records	§ 820.170	Inspection records
§ 820.30	Design control documentation	§ 820.75	Validation records	§ 820.181	DMRs
§ 820.40	Controlled documents	§ 820.80. § 820.90	QC records	§ 820.184	DHRs
§ 820.50	Supplier quality records	§ 820.86	Acceptance records	§ 820.186	QSR
§ 820.60 § 820.140 § 820.150	Inventory management	§ 820.100	CAPA records	§ 820.198	Complaint Management Systems
§ 820.65	DHRs	§ 820.120	Label control and inspection records	§ 820.200	Service reports

21 CFR Part 11: Considerations for Cloud Systems

- Security:
  - Security for the datacenter should be considered and periodically audited by the quality unit
- Data availability:
  - ISP selection should have some justification, uptime guarantees per SLA
  - Backup and recovery must be implemented and tested
- Data confidentiality
  - Virtual machine architecture must be coupled with access controls at the management level and service provider agreements, as appropriate.
- Data integrity controls when data travels outside the qualified infrastructure:
  - Data in transit, offsite backup, system maintenance: The controls put in place here will address Part 11's requirements for open systems
- Data and system segregation:
  - How is data from that of other systems/customers. In a colocation environment, regulated companies should consider the risks when resources are shared

21 CFR Part 11: Some Specific Requirements

§11.1(e) Computer systems (including **hardware and software**)…shall be readily available for, and subject to, FDA inspection.

- Cloud systems must be **auditable** if they store electronic records that are subject to predicate rules

§11.30 Controls for open systems: Persons who use open systems…shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records

- The preamble to Part 11 indicates that systems hosted by a third party are considered open systems. System validation should **address integrity controls for data at rest and in transit**

- **§11.300 (d)** Controls for identification codes/passwords: Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.
  - **Identification** procedures, **authentication** mechanisms, system **monitoring** tools and access **logs**

High Level Risk Mitigations for Cloud Computing

- **System qualification** (to reduce the risk of improper installation, configuration, and operation)
- **System maintenance** (including preventive maintenance, change control, incident management, CAPA processes, procedures, training, and ongoing monitoring), to reduce the risk of, and respond to, system failures
- **Access restrictions**, policies, procedures and training to reduce the risk of unauthorized modification of data and system components

Risks to Data Integrity: Facilities/physical utilities

- **System failure** damages higher level elements, such that data is temporarily unavailable or permanently lost (e.g. improper environmental conditions)
- **Inappropriate access** permits unauthorized modification that compromises these systems, resulting in data loss or data corruption.
- **Inappropriate access** permits inappropriate access to higher level elements (e.g. inappropriate access to servers), resulting in data loss, data corruption, or unauthorized data modification or disclosure.

Risks to Data Integrity: Network, storage, and management infrastructure

- **System failure** restricts data availability
- **Improper configuration** permits unauthorized access, resulting in data loss/corruption, unauthorized disclosure or unauthorized data modification.
- **System failure** results in data loss or data corruption (e.g. drive failure, introduction of malicious software).
- **Inappropriate access** results in data loss or corruption or unauthorized data modification.

Risks to Data Integrity: Applications

- **System failure** or **inappropriate access** leads to a failure of supporting processes that affects other platform elements. Risks associated with these elements are not mitigated.
- **Inappropriate access** allows unauthorized modification, resulting in data loss/data corruption.
- **Inadequate design** allows records to be modified in appropriately, audit trail lacking or non-existent, eSignature requirements unmet

Risks to Data Integrity: Processes and People

- **Process failures** mean that platforms are not implemented, maintained or managed correctly. Platforms don't operate or perform as required, resulting in data loss, data corruption, or unauthorized data modification
- **Personnel failure** means processes are not implemented and managed correctly. Platform elements are adversely impacted, resulting in data loss, data corruption or unauthorized data modification.
- **Responsibilities** not well defined
- **Multiple QMS** acting as one. If not well planned, compliance gaps are possible.

Validating Cloud-Based Applications

Application
Software V&V, Monitoring & Maintenance, Client side qualification, Training

Application Platform
Virtual Environment, Databases, Backup and Restore, Disaster Recovery, Network Security, Identification/Authentication, Monitoring and Maintenance

Computing Environment
Physical Servers, Network Components, Virtual Environment, Logical Security, Monitoring & Maintenance, Training, Disaster Recovery, Backup and Restore

Facility
Utilities, Physical Security, Logical Security, Monitoring and Maintenance, Training, Disaster Recovery

21 CFR 820.50 Requirements for Outsourced Systems

Evaluate and select potential suppliers, contractors, and consultants on the basis of their ability to meet specified requirements, including quality requirements.	• Audit facilities, procedures, and processes • Demonstrate readiness for regulatory audits • Implement documented policies and procedures to define how quality is controlled and assured • Help device manufacturers establish traceability from their specified requirements to the cloud hosting providers services
Define the type and extent of control to be exercised over the product, services, suppliers, contractors, and consultants, based on the evaluation results.	• Implement documented procedures to ensure consistent delivery of required services • Establish a clear SLA to guarantee that services are provided with the required level of control
Establish and maintain data that clearly describe or reference the specified requirements, including quality requirements, for purchased or otherwise received product and services. Purchasing documents shall include, where possible, an agreement that the suppliers, contractors, and consultants agree to notify the manufacturer of changes in the product or service so that manufacturers may determine whether the changes may affect the quality of a finished device.	• Include change notification requirements in the SLA • Maintain rigorous, well-documented change control procedures, to ensure that all changes are reviewed, approved, tested and implemented as required for device quality, and with the device manufacturer's approval • Allow periodic audits to confirm ongoing compliance

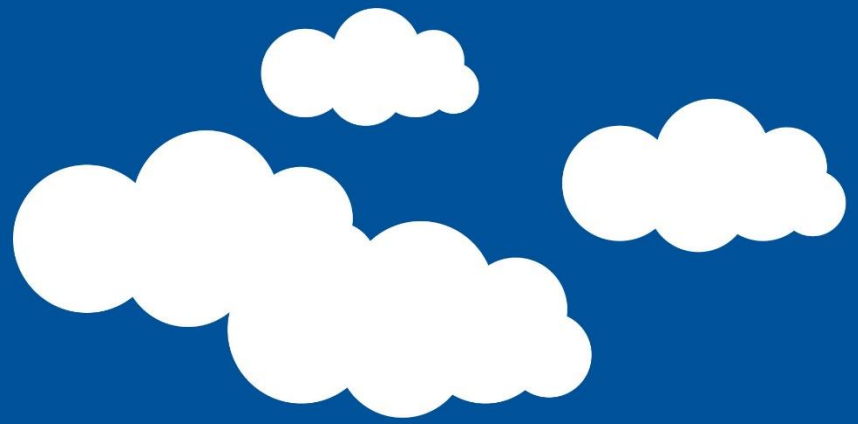
Traditional Infrastructure Controls

- Infrastructure Qualification
- Change management
- Configuration management
- Security Management
- Client management
- Network Management
- Problem Management
- Support/Help Desk
- Backup, Restore and Archiving
- Disaster Recovery
- Performance Monitoring
- Supplier Management
- Periodic Review
- Retirement Management

Cloud Controls

- Service Level Agreement (I/P/S)
- Validation & Qualification (I/P/S)
- Data Privacy (I/P/S)
- Quality Agreement (I/P/S)
- Data Segregation (I/P/S)
- Change Management (I/P/S)
- Configuration Management (I/P/S)
- Security Management (I/P/S)
- Server Management (I/P/S)
- Client Management (I/P/S)
- Network Management (I/P/S)
- Problem Management (I/P/S)
- Problem Management (I/P/S)
- Help Desk (I/P/S)
- Backup, Restore, and Archiving (I/P/S)
- Disaster Recovery (I/P/S)
- Performance Monitoring (I/P/S)
- Supplier Management (I/P/S)
- Periodic Review (I/P/S)
- Retirement of Platforms (I/P/S)
- SDLC Standards (S/P)
- All Controls Shared
  - I: IaaS
  - P: PaaS
  - S: SaaS

GXP CLOUD USE CASES



Use Case - SaaS - CRO - EDC

- CRO's use Electronic/Remote Data Capture Systems to capture study information for clinical
- Depending on the size of the CRO an E/RDC system can be used to manage a couple of dozen to a couple of hundred studies at any one time.
- Systems accessible anywhere an internet connection exists, opportunities for globally dispersed study sites
- IT support is product dedicated
- Highly sensitive data with huge patient safety implications. Where is it stored? Who has access?
- Even partial loss of CRF data can invalidate a study
- Data entry conducted via browser (varied security/compatibility issues)
- Who controls and qualifies core configuration of application?

Use Case - SaaS - Mfg - ERP

- Enterprise Resource Planning systems are used by manufacturers to electronically manage inventory, the order to cash process, QA/QC hold's, distribution, recall's and even product recipes
- Most ERP systems are now offered in a SaaS configuration
- Significant hardware savings
- Every PC/device becomes a process control interface
- Real-time access to Quality & Production data anywhere anytime
- Must consider diverse input device strategies
- Large data loads
- System uptime must be 100%

Use Case - SaaS - Lab - LIMS

- LIMS systems widely used in industry
- A traditional in-house, client/server-based LIMS can cost a pharmaceutical company anywhere from $250,000 to several million dollars in start-up costs, consulting, customization, licensing fees, and ongoing maintenance.
- In the SaaS model $10-$20k plus a nominal monthly fee can deliver the same product
- Reduces number of spreadsheets in use
- Affordable for small labs
- Increased data quality
- No need to have specialized staff on team
- Will require rigid SLA for configuration management
- Difficult to troubleshoot instrument connection issues
- Many lab instruments ship with their own PC’s and lack corporate security and anti-virus protection

Use Case - XaaS – MedDev Mfg- Cloud

- Personalized medicine driving cloud product
- Implantable devices can transmit status
- Real-time emergency care
- Possibility for automated care
- Medical Device data being sent over the public airways
- Huge data needs - Where is it being stored
- Unknown/unclear impact of radio emitting devices
- Data Privacy concerns (HIPAA/HITECH)
- Highly complex validation required to fully understand the impact of late/partially received commands/warnings

References

- 21 CFR Part 11 – Electronic Records; Electronic Signatures, US Code of Federal Regulations, US Food and Drug Administration (FDA)
- 21 CFR Part 820 – Quality System Regulations, US Code of Federal Regulations, US Food and Drug Administration (FDA)
- MHRA GMP Data Integrity Definitions and Guidance for Industry Revision 1.1, March 2015
- Data Integrity and Compliance with CGMP, Guidance for Industry, DRAFT GUIDANCE, US Food and Drug Administration (FDA), April 2016
- Eudralex Vol. 4, Annex 11, Computerised Systems
- Process Validation: General Principles and Practices, Guidance for Industry, US Food and Drug Administration (FDA), January 2011
- GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, ISPE, 2008
- Considerations for a Corporate Data Integrity Program, ISPE GAMP Community of Practice, March 2016
- Data Integrity, Parenteral Drug Association, Ireland Chapter, 12th May 2015,
- Cloud Compliance: Benefits, Risks & Challenges in the FDA Regulated Domain, Stephen Ferrell, 2015

QUESTIONS?