Partially Cloudy
With a Chance of Value

Dan Ringenbach

Sr. Enterprise Architect, R&D Information, AstraZeneca

-Worked at AstraZeneca for 15 years in IT and clinical development.

- Enterprise Architecture
- Information Strategy

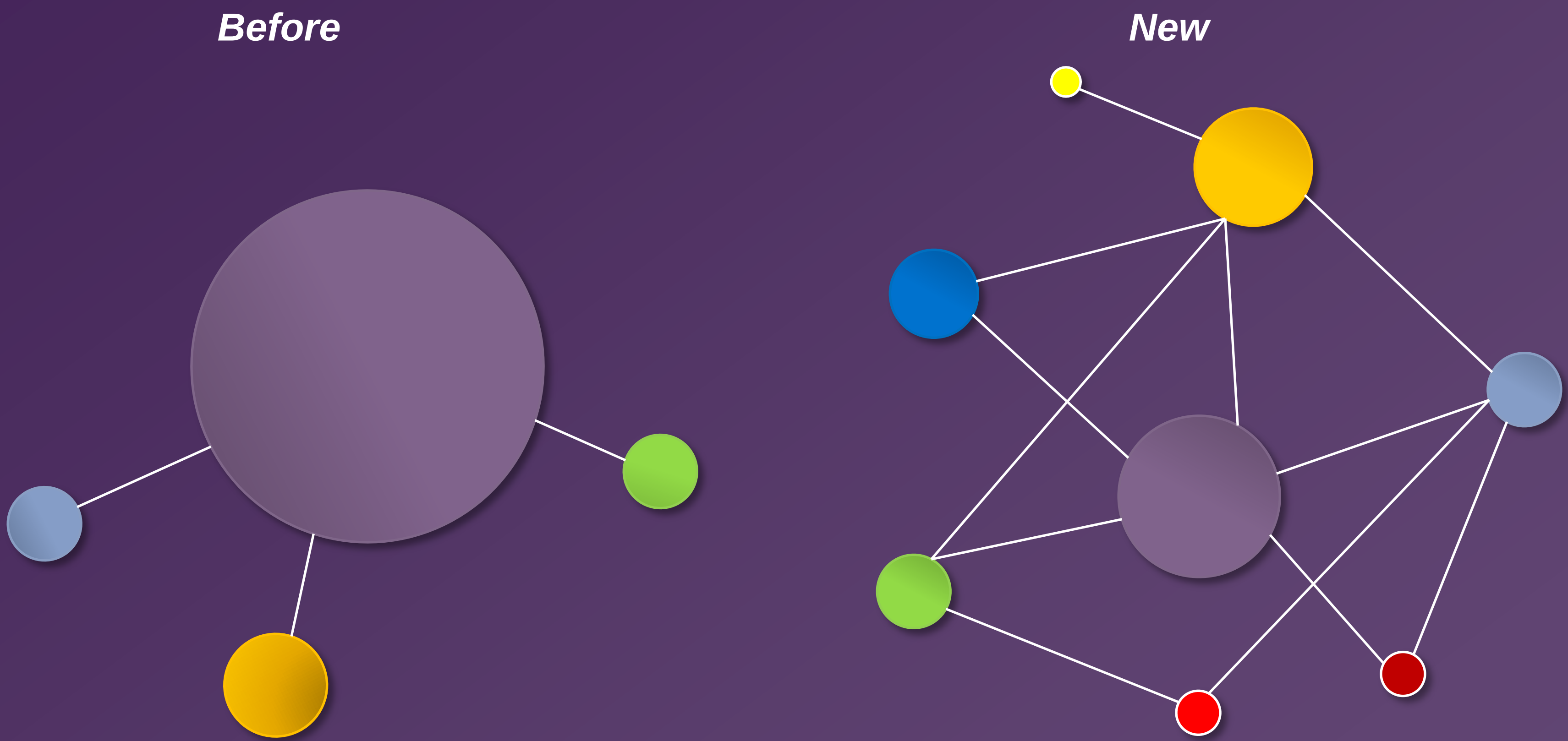
AstraZeneca

Agenda

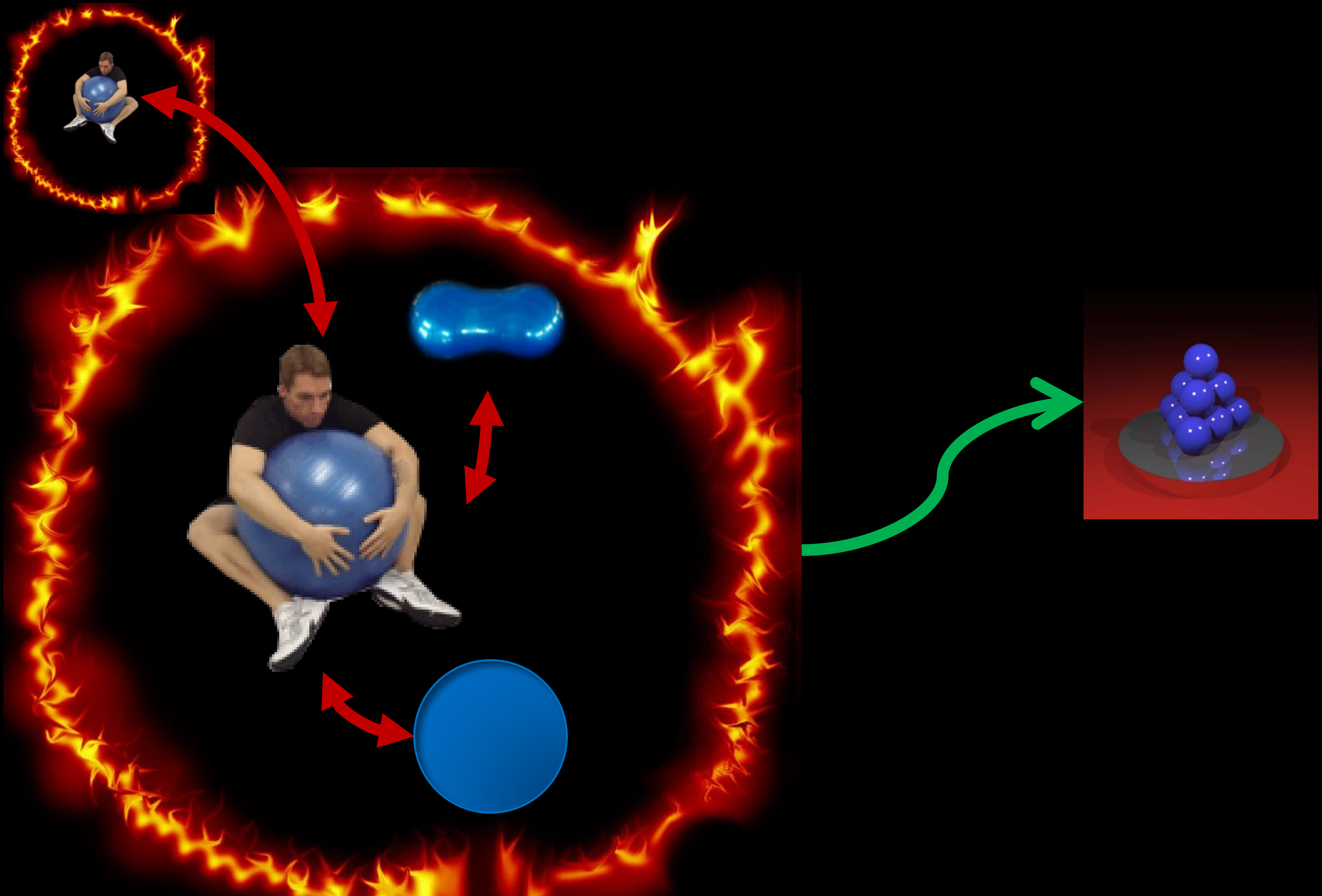
- Challenge
  - New Business Model
  - New business challenges
- Turning to the Cloud in a Solution
- Considerations
  - Security, Privacy
- AZ Neuro Cloud Based Clinical Repository
- Benefits / Value
- Future

THE CHALLENGE

Like it or Not, There is a New Business Model

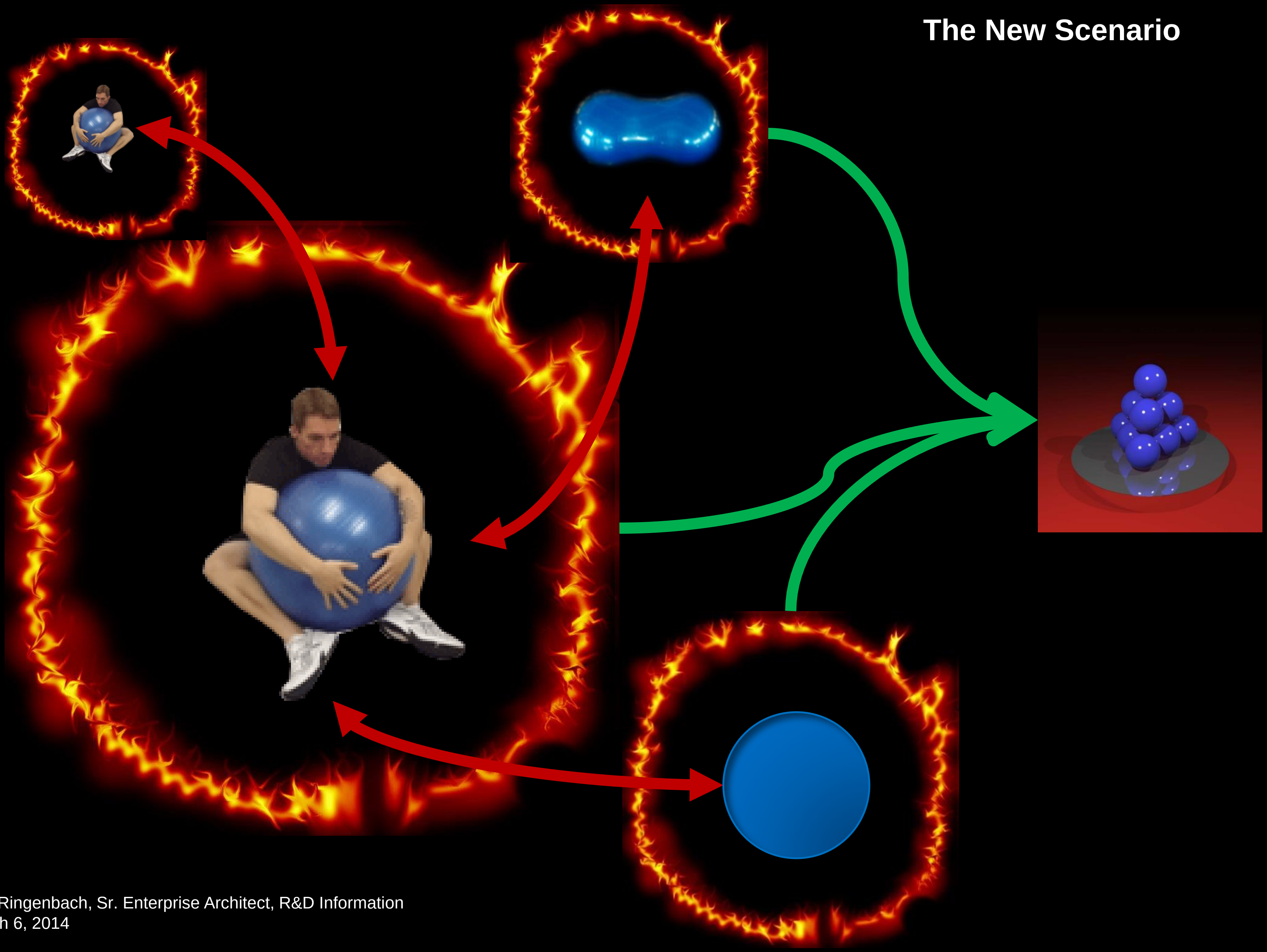


The Old Scenario



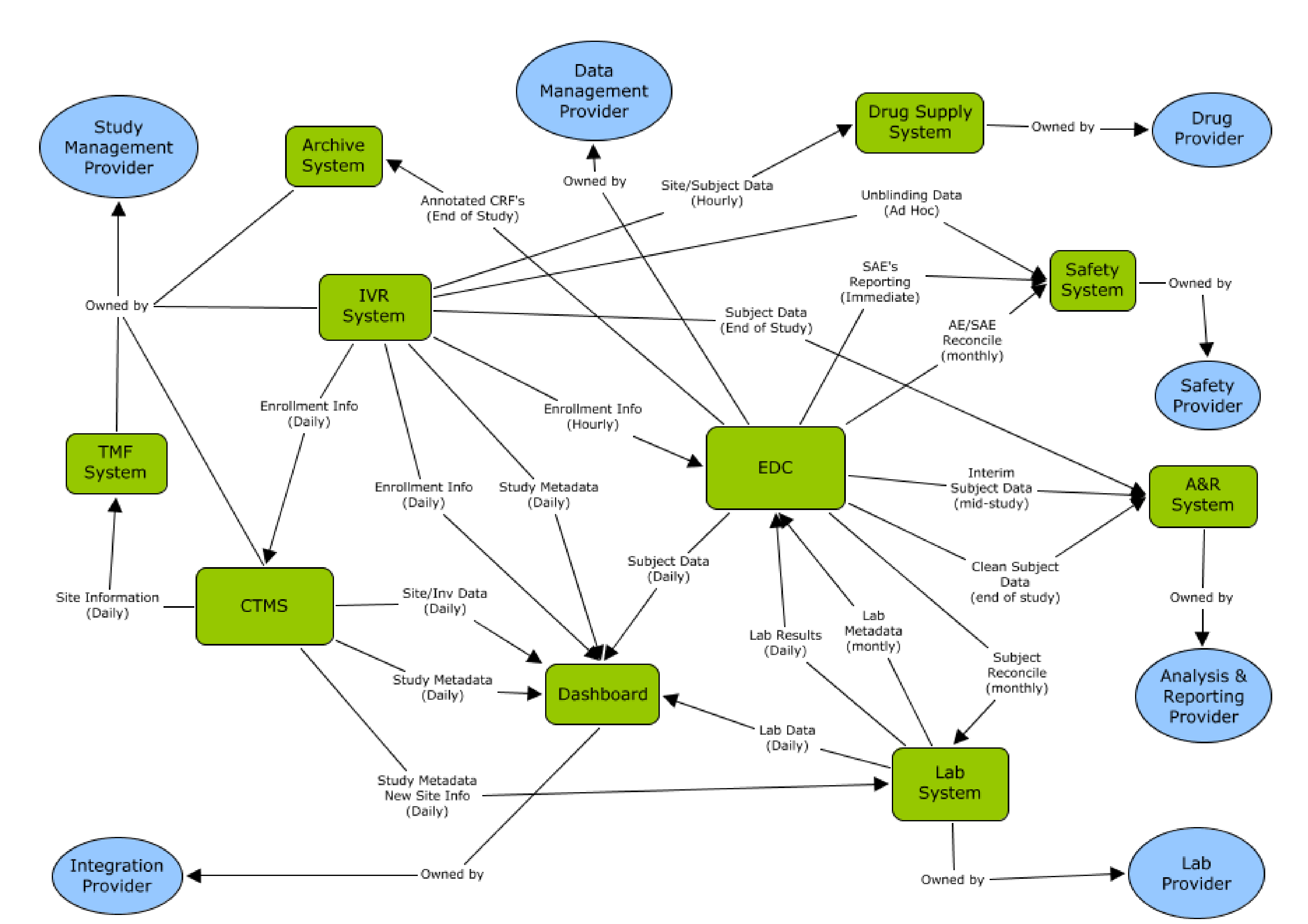
Dan Ringenbach, Sr. Enterprise Architect, R&D Information
March 6, 2014

The New Scenario



Dan Ringenbach, Sr. Enterprise Architect, R&D Information
March 6, 2014

Information Exchange in a Trial



Dan Ringenbach, Sr. Enterprise Architect, R&D Information
March 6, 2014

Information Explosion

- Electronic Health Records

- Real World Evidence Databases

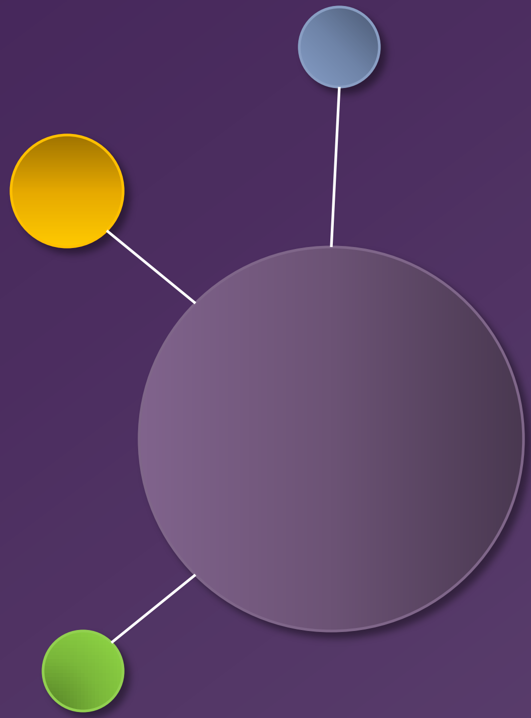
- Social Networking / Blogs

patientslikeme®

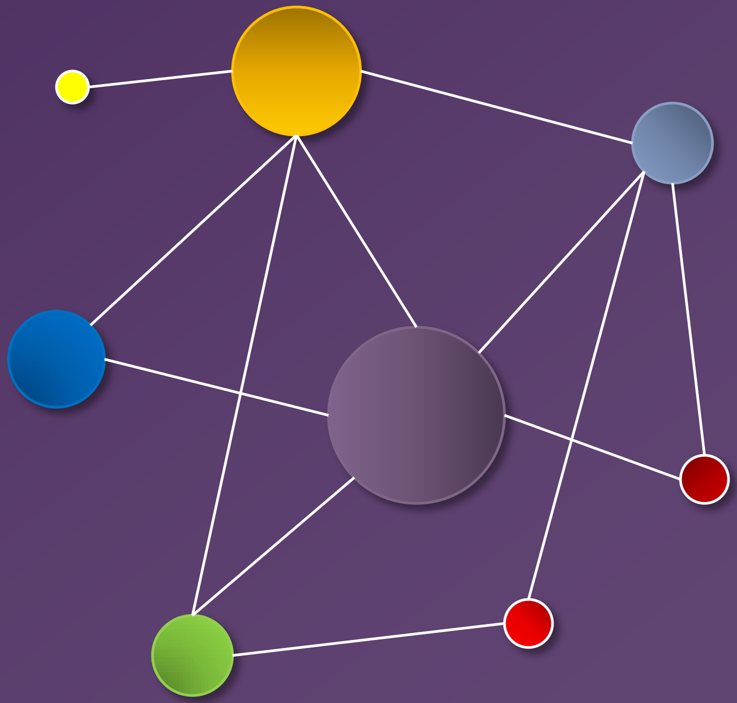
- Patient Groups

Like it or Not, There is a New Business Model

Before



New



Cloud solutions enable a distributed business model
…the question is "why would you not leverage the cloud?"

TURNING TO CLOUDS AS A SOLUTION

Cloud Acronyms & Definitions

SaaS

Software-as-a-service is a model of software **deployment whereby a provider licenses an application to customers for use as a service.**

IDaaS

Identity-as-a-service refers to the practice of **delivering identity management as a service.**

PaaS

Platform-as-a-service refers to **delivering a platform or entire environment as a service. (**operating system, programming language, database, and web server)

IaaS

Infrastructure-as-a-service is the delivery of **computer infrastructure as a service.**

OpenID

An open, decentralized, free framework for a user-centric digital identity. OpenID eliminates the need for multiple usernames across different websites, simplifying your online experience.

SAML

Security Assertion Markup Language is an **XML-based standard for exchanging authentication and authorization data between security domains—that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions).**

Two-factor Authentication

Two different factors are used in conjunction to authenticate individuals.

IdP

An *identity provider is a service provider* that creates, maintains, and manages identity information and asserts identities to other service providers within a federation.

OAuth

An open authorization protocol standard lets users give third-party websites limited access to data without giving away passwords. The protocol enables websites or applications (consumers) to access protected resources from web services (SP) via an API, without requiring users to disclose their SP credentials to those consumers.

Public Cloud

A cloud service that is hosted, operated, and managed by a third-party vendor from one or multiple data centers, and offered to multiple customers.

Hybrid cloud

An environment of internal or external providers where an organization run non-core applications in a public cloud, while maintaining core apps and sensitive data in a private cloud.

Private cloud

An offering that emulates public cloud computing, but on a private network.

HIPAA

The *Health Insurance Portability and Accountability Act was enacted by the U.S.* Congress in 1996 and requires entities that process protected health information to comply with security and privacy requirements.

SAFE HARBOR

A policy agreement between the U.S. Dept of Commerce and the European Union (E.U.) in Nov. 2000 to regulate the way that U.S. companies export and handle the personal data of European citizens.

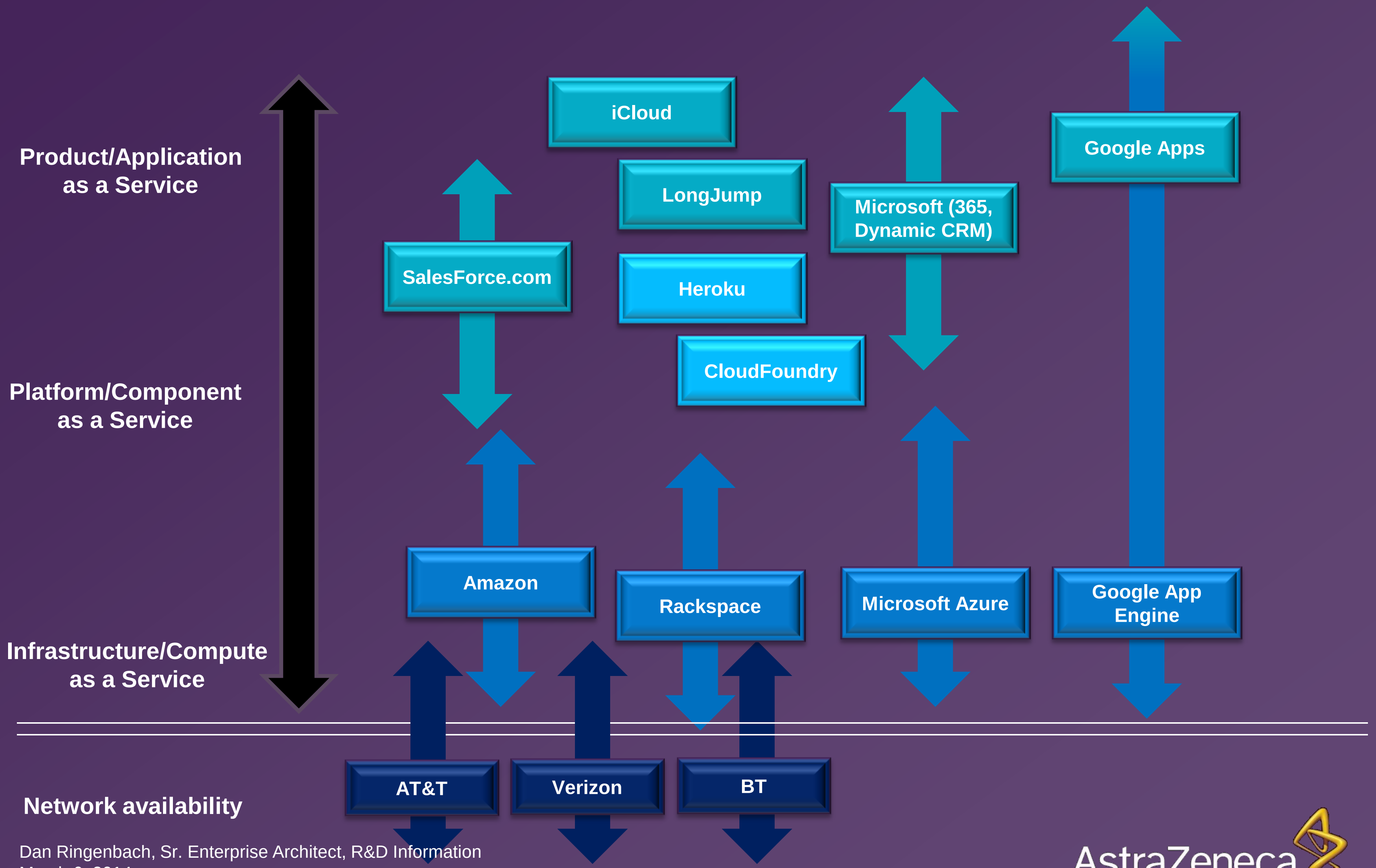
PII

Personally identifiable information

Dan Ringenbach, Sr. Enterprise Architect, R&D Information
March 6, 2014

AstraZeneca

Cloud Examples



Product/Application as a Service

Platform/Component as a Service

Infrastructure/Compute as a Service

Network availability

Dan Ringenbach, Sr. Enterprise Architect, R&D Information
March 6, 2014

AstraZeneca

Why/when not to use the cloud?

Replacing an Existing system with a complex integration scheme (e.g. poor de-coupling)

- Although a cloud solution can be the path to cleaning up the application landscape moving one application at a time with the use of proper de-coupling technologies (e.g. SOA)

Total Cost of Ownership – is it economically viable

- Total cost of a private cloud for regulatory system is more costly than total cost of ownership (if internal managed & hosted)
- Consistent need for a given level of compute power (e.g. HPC) and total cost of cloud solution is more costly than TCO

Content or software license prohibits the cloud

There are simply no cloud offering in the space

Risk vs benefit of move is not worth it

CONSIDERATIONS
PRIVACY & SECURITY

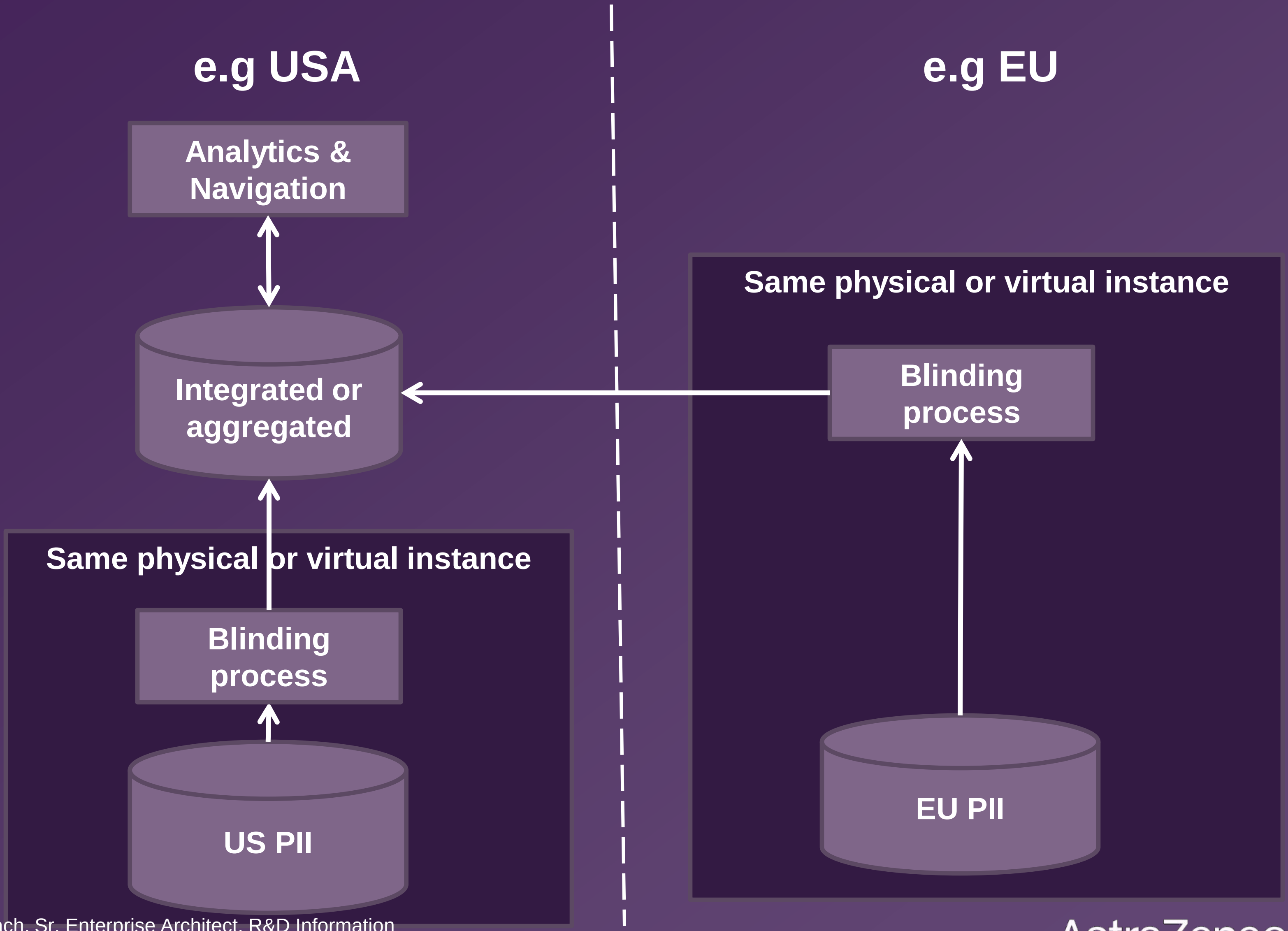
What is privacy?

The concept varies widely among (and sometimes within) countries, cultures, and jurisdictions.

Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data (or personally identifiable information—PII).

Organizations are accountable to data subjects, as well as the transparency to an organization’s practice around personal information.

Satisfying PII *transfer principle*



Dan Ringenbach, Sr. Enterprise Architect, R&D Information
March 6, 2014

AstraZeneca

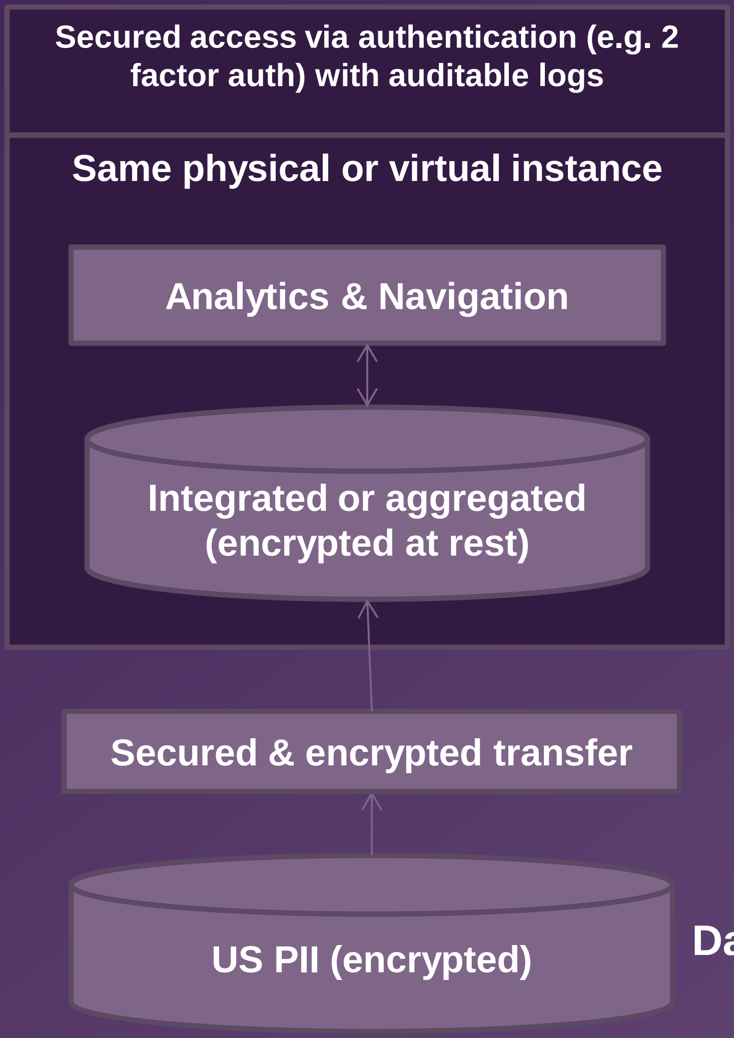
Data Security

When it comes to the security of data stored in a public cloud, you have two potential concerns:

1. What access control exists to protect the data?
   - Solution: Access control consists of both authentication and authorization.
2. How is the data that is stored in the cloud actually protected?
   - For all practical purposes, protection of data stored in the cloud involves the use of encryption.

- The data should be encrypted at rest and in transit

Satisfying PII Security



Secured access via authentication (e.g. 2 factor auth) with auditable logs

Same physical or virtual instance

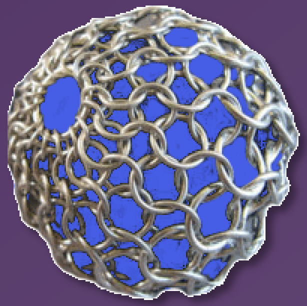
Analytics & Navigation

Integrated or aggregated (encrypted at rest)

Secured & encrypted transfer

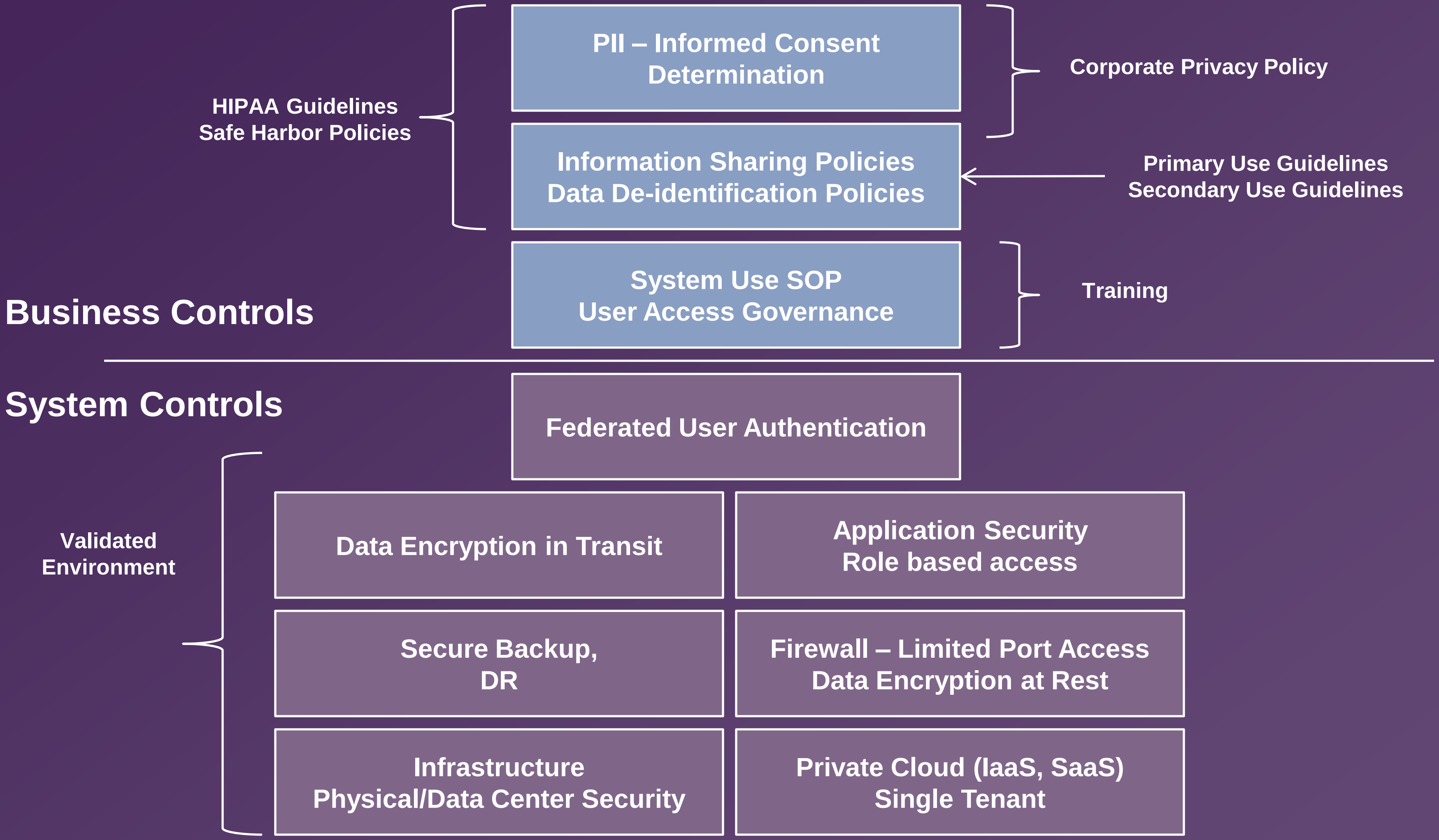
US PII (encrypted)

Data gathered under consent



PII = personally identifiable information

Security and Privacy Controls



HIPAA Guidelines
Safe Harbor Policies

PII – Informed Consent Determination

Corporate Privacy Policy

Information Sharing Policies
Data De-identification Policies

Primary Use Guidelines
Secondary Use Guidelines

Business Controls

System Use SOP
User Access Governance

Training

System Controls

Federated User Authentication

Validated Environment

Data Encryption in Transit

Application Security
Role based access

Secure Backup,
DR

Firewall – Limited Port Access
Data Encryption at Rest

Infrastructure
Physical/Data Center Security

Private Cloud (IaaS, SaaS)
Single Tenant

Dan Ringenbach, Sr. Enterprise Architect, R&D Information
March 6, 2014

AstraZeneca

AZ NEURO CLOUD BASED CLINICAL REPOSITORY

AZ Neuro Clinical Repository

Application

- Low Cost
- Store Data & Documents
- Validated - Part 11 Compliant
- Off-the Shelf Software
- Quick Delivery

Uses

- Ad Hoc Reports
- Cross-Trial Data Pooling
- Enforce Data Sharing Policies
- Complex Custom Reports
- Role Based Access
- Access & Share Data
- Visualize Data
- Cohorts & Datamarts
- Use with SAS, Spotfire

Inputs

- Legacy Trial Data
- Multiple Projects & CRO's
- Analysis Data & Models
- On-going Trial Data (blinded)
- Trial Documents CSP, ICF etc

AZ Neuro

MAXISIT® Integrated Clinical Development Platform

Repository

Architecture

- Cloud Based
- Single Sign-on
- Anywhere Web Access
- Encrypted At rest & In-flight
- Performance & Scalability
- Maintain Data Privacy

Service

- Export Data To AZ
- Search Data & Documents
- Clinical Data Services
- IT Support Services

Standards

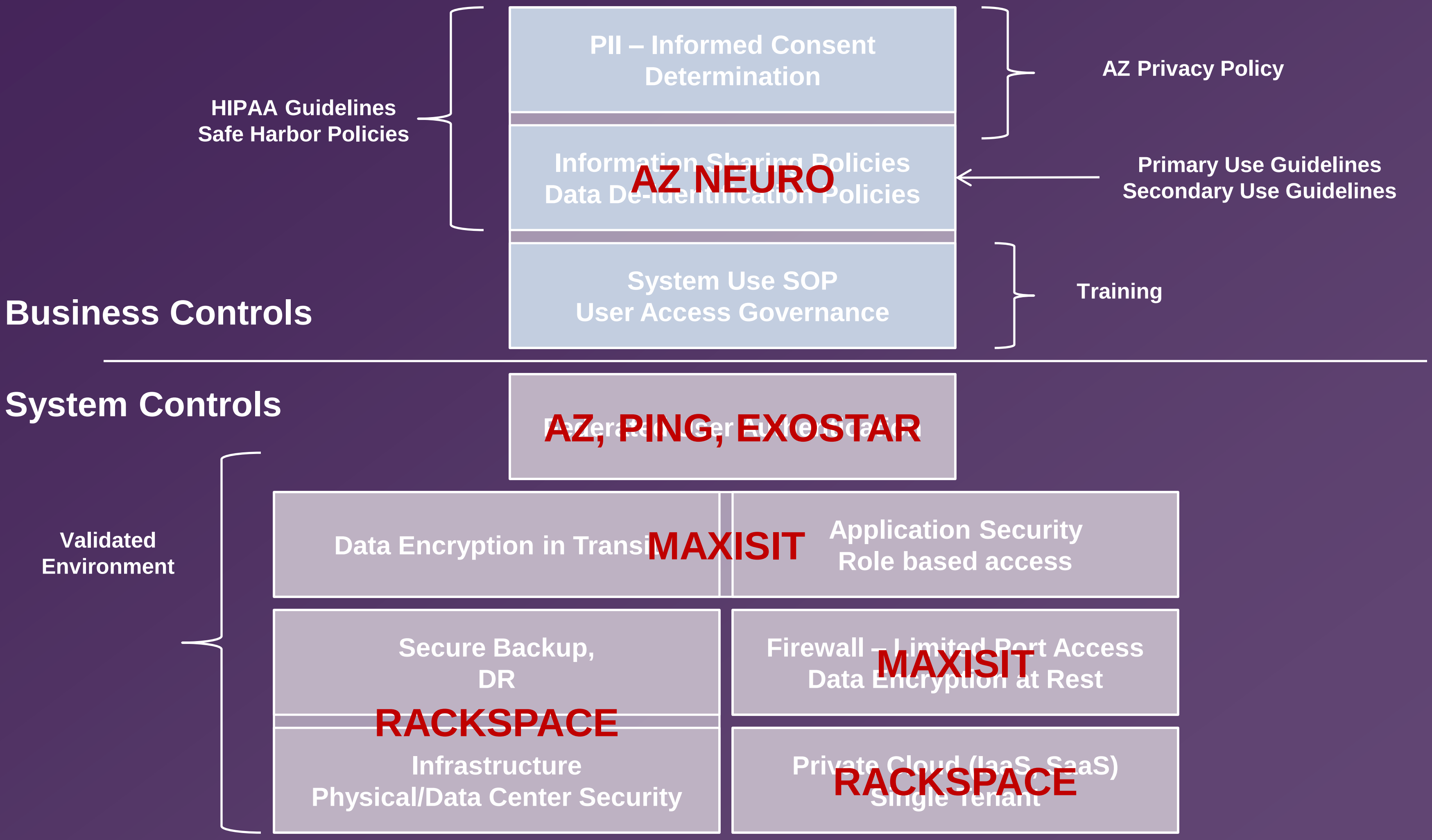
- SDTM, eTMF, MedDRA AZDD
- Use of Industry Data Standards

AstraZeneca

Solution Selection

- MAXISIT Partnering
  - Global organization with 10 plus years experience in delivering integrated solutions for pharmaceutical and life sciences industry companies
  - Strong partnership with strong involvement for business specification
- CTRenaissance® eXchange
  - Industry leading Integrated Clinical Data Management Platform with required functionalities available out-of-the-box
  - Flexible delivery models and global strength to support scalable needs

Security and Privacy Controls



HIPAA Guidelines
Safe Harbor Policies

PII – Informed Consent
Determination

AZ Privacy Policy

Information Sharing Policies
Data De-identification Policies

AZ NEURO

Primary Use Guidelines
Secondary Use Guidelines

System Use SOP
User Access Governance

Training

Business Controls

System Controls

Federated User Authentication

AZ, PING, EXOSTAR

Validated
Environment

Data Encryption in Transit

MAXISIT

Application Security
Role based access

Secure Backup,
DR

RACKSPACE

Firewall – Limited Port Access
Data Encryption at Rest

MAXISIT

Infrastructure
Physical/Data Center Security

Private Cloud (IaaS, SaaS)
Single Tenant

RACKSPACE

AstraZeneca

Data Encryption in Transit

- AZ Neuro CDR application is secured and enables access to only authenticated and authorized users.
- Accessible only over https.
- High-grade encryption used (TLS_DHE_RSA_WITH_AES_256_CBC_SHA, 256 bit keys)
- All the pages which users are able to view are encrypted before being transmitted over the internet.
- This will secure the encryption in transit from application to client browser.

Data Encryption in Rest

- Application is deployed in a secured hosting environment and behind the firewall with only port 443 (https) being enabled.
- Internal communications are originated and ended in a secure zone and no information is encrypted from one service to another service.
- For data storage, the application uses a MySQL database to store the transactional and asset related data and an Oracle database to store the clinical and analytical data
- The data is not encrypted at the database level.
- The content which is stored into the Repository will be encrypted by default and therefore can't be accessed directly by any user.

Data Encryption at Rest

- For all the data backups Data Hosting includes AES256-GCM encryption to all (Linear Tape Open); LTO-based tape media to be shipped to offsite media vaults.
- Data Hosting ensures that all media sent offsite is shipped in locked, water-resistant and impact-resistant containers in order to protect the media from tampering, dropping or exposure to extreme environmental elements.
- Offsite vendor representatives do not have direct access to individual media containing customer data at any point or any time during the transport container’s offsite period.

BENEFITS - VALUE

Potential Benefits of Cloud

- Cost
  - Reduced software license cost
  - Reduced hardware hosting costs
- Speed
  - Reduced hardware procurement and qualification time
  - Reduced trial startup time
- Quality
  - Increase in data quality
- Supports decoupled systems, API's, web services

Potential Benefits of Cloud

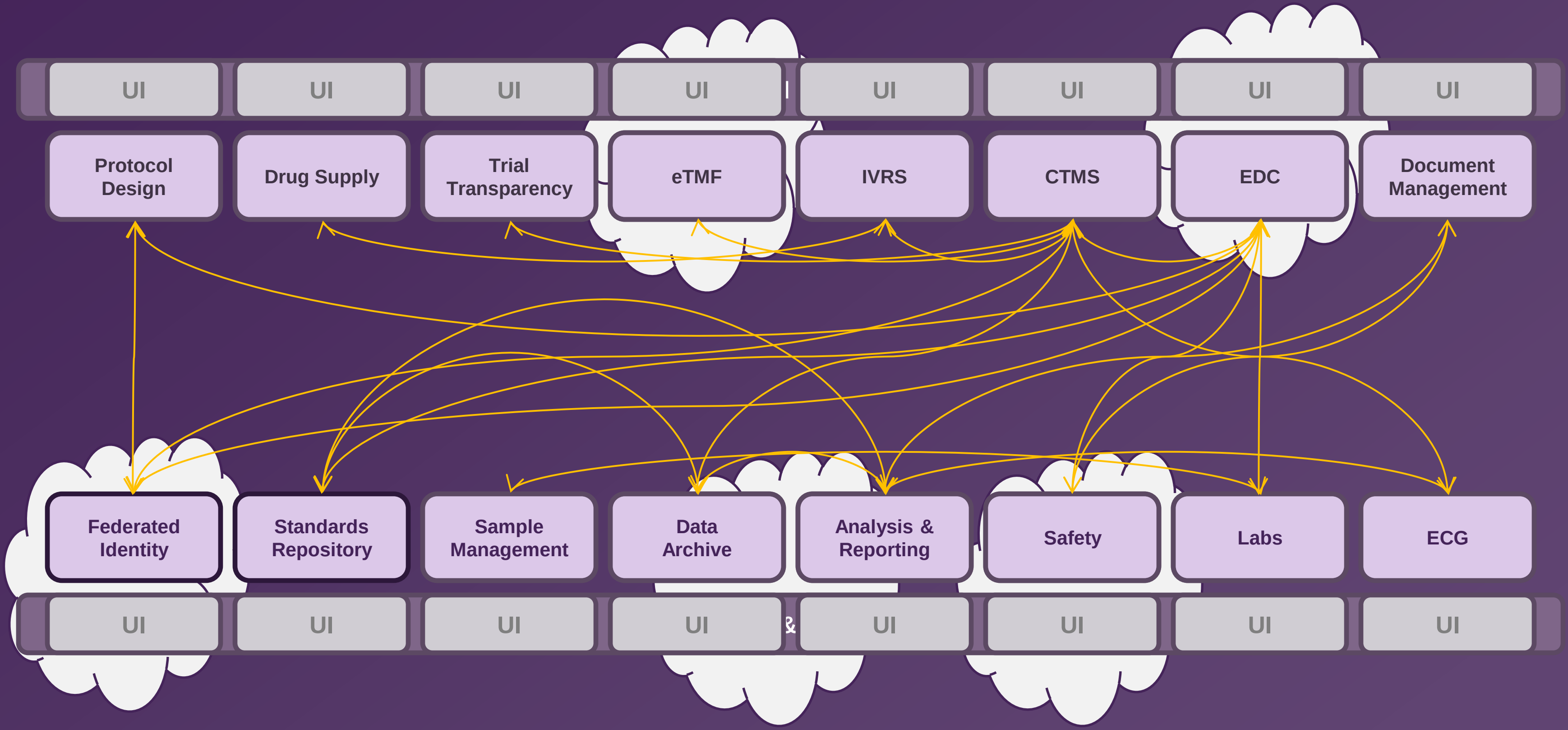
- Maintenance
  - Less customized technology and legacy systems
  - Low footprint or no footprint applications
- Scalability
  - Add additional storage or compute power as demand increases
- Virtualization enabled by cloud
  - Ease of migration from one server to another
  - Increased usage of resources
- Location Independence
  - Access from anywhere

FUTURE

Clinical Cloud Platform Future Vision

- Facilitate a federated environment of interchangeable components where clinical information is easily and readily exchanged and is semantically interoperable both internally and externally with partners in a system-independent format that meets regulatory requirements for electronic data handling and archiving.

Multiple Clouds in the Landscape



UI UI UI UI UI UI UI UI

Protocol Design

Drug Supply

Trial Transparency

eTMF

IVRS

CTMS

EDC

Document Management

Federated Identity

Standards Repository

Sample Management

Data Archive

Analysis & Reporting

Safety

Labs

ECG

UI UI UI UI UI UI UI UI

Dan Ringenbach, Sr. Enterprise Architect, R&D Information
March 6, 2014

AstraZeneca

The Cloud is Growing

Identity

Innovation/Find

Collaboration/Engage

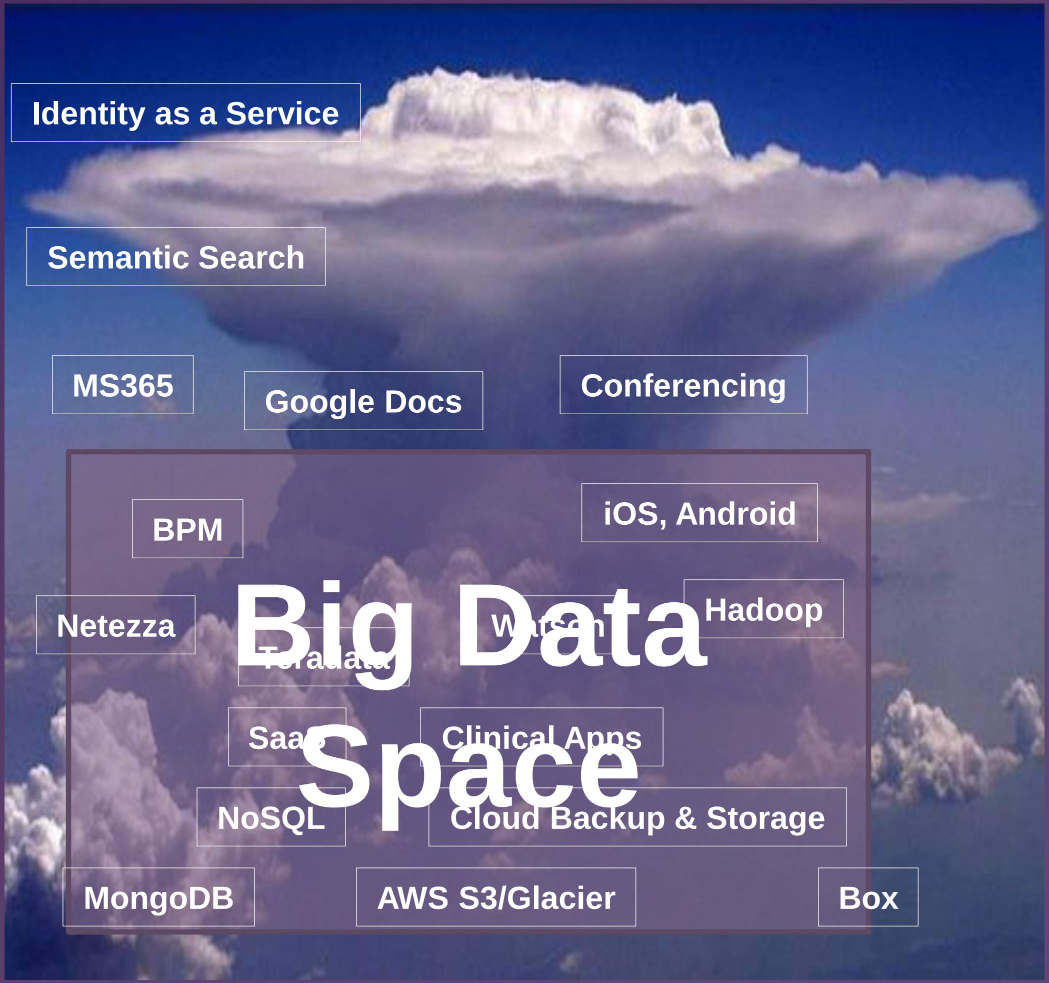
Device (App Store)/Deliver

Orchestration/Plan

Analytics/Predict

Process/Execute

Storage Content/Results



Identity as a Service

Semantic Search

MS365

Google Docs

Conferencing

BPM

iOS, Android

Big Data Space

Netezza

Watson

Hadoop

Teradata

SaaS

Clinical Apps

NoSQL

Cloud Backup & Storage

MongoDB

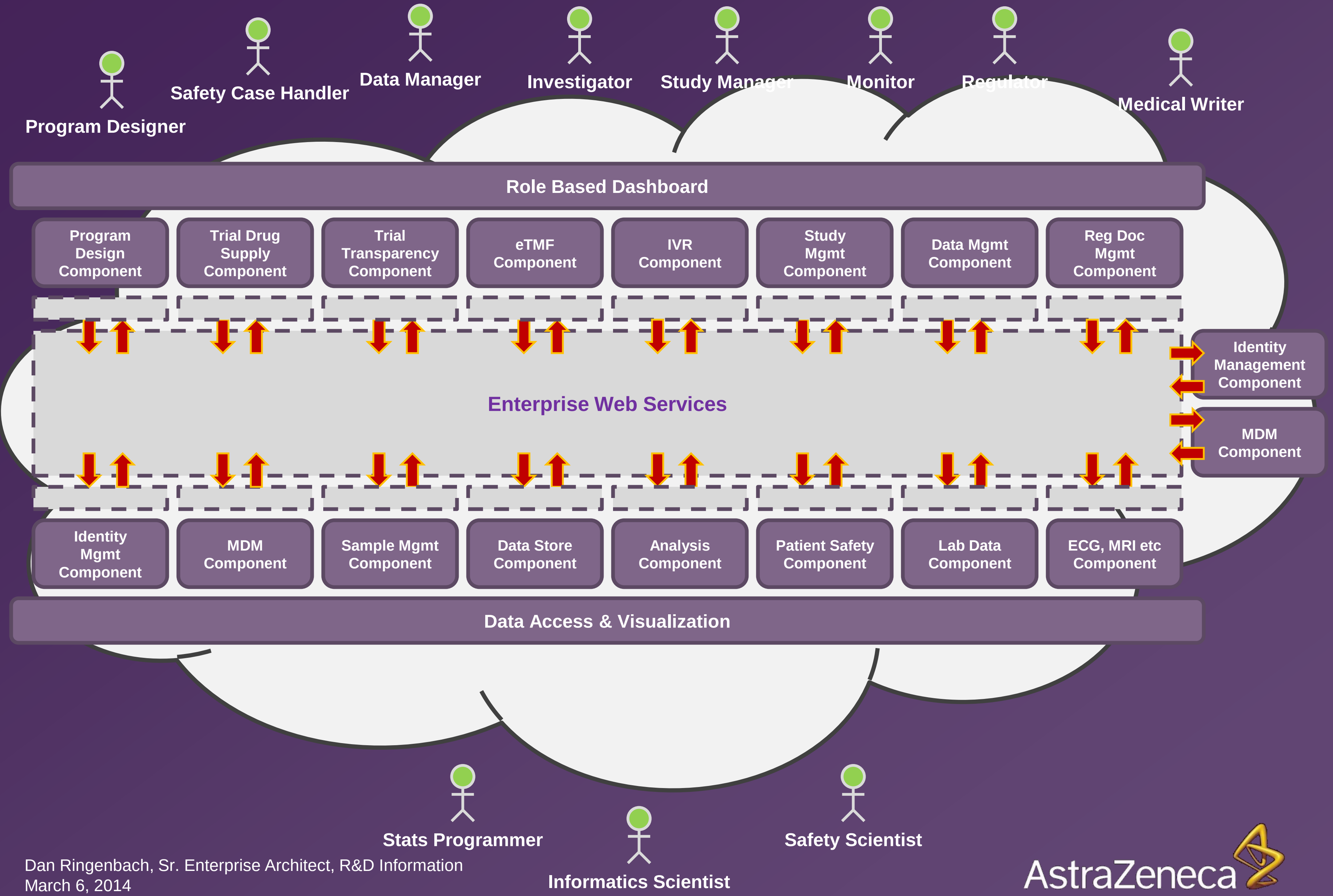
AWS S3/Glacier

Box

Dan Ringenbach, Sr. Enterprise Architect, R&D Information
March 6, 2014

AstraZeneca

Future Conceptual Landscape



Program Designer

Safety Case Handler

Data Manager

Investigator

Study Manager

Monitor

Regulator

Medical Writer

Role Based Dashboard

Program Design Component

Trial Drug Supply Component

Trial Transparency Component

eTMF Component

IVR Component

Study Mgmt Component

Data Mgmt Component

Reg Doc Mgmt Component

Enterprise Web Services

Identity Management Component

MDM Component

Identity Mgmt Component

MDM Component

Sample Mgmt Component

Data Store Component

Analysis Component

Patient Safety Component

Lab Data Component

ECG, MRI etc Component

Data Access & Visualization

Stats Programmer

Informatics Scientist

Safety Scientist

Dan Ringenbach, Sr. Enterprise Architect, R&D Information
March 6, 2014

AstraZeneca

Challenges

- Speed of Technology Change faster than business project cycles
  - Outdated before implemented
- Speed of Regulatory Guidance leaves risk in adopting new technologies
- Assessing Risks in Privacy & Security
- Return on Investment – Does all this technology actually translate into better decisions, faster development?
- Data retention, control and access
- Mergers & Acquisitions

Questions?

Dan Ringenbach
daniel.ringenbach@astrazeneca.com

Confidentiality Notice