Yellow Schedule

Security Whitepaper

This document provides information about the security, encryption, backup processes of Yellow Schedule

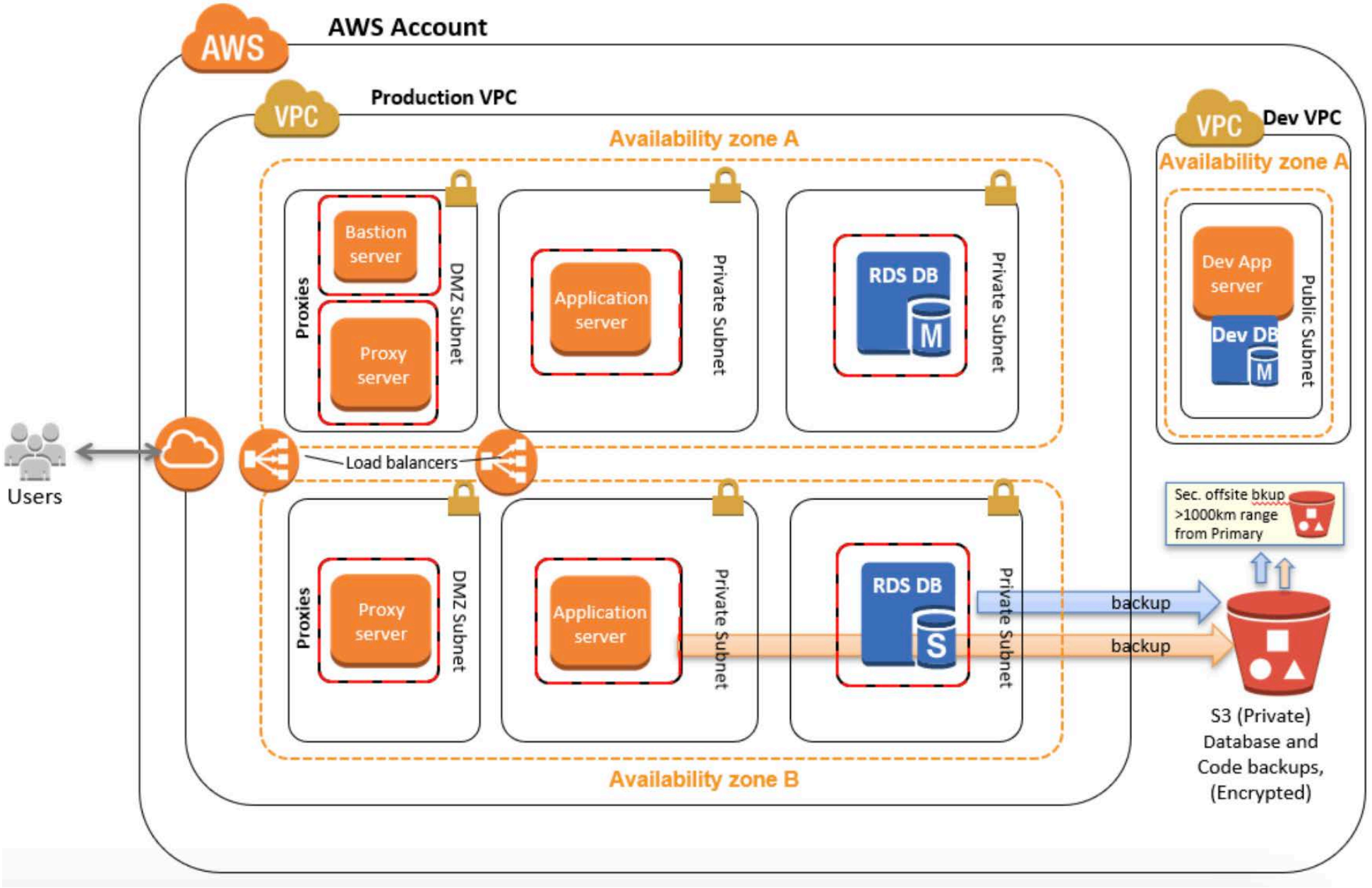
Security at Scale: Hosted on highly available AWS infrastructure, over 25 million client appointments have been created on the system. Tens of millions of dollars in client payments have been gathered and transferred to customers. Tens of millions of individual patient communications have been facilitated, millions of secure API requests to our servers and more recently the platform has supported hundreds of thousands of hours of confidential video communications between practitioners and patients.

Please see the system architecture diagram posted below that supports and facilitates our platform.

SUMMARY

1

Architecture / Schematic


AWS
AWS Account
VPC
Production VPC
Availability zone A
Bastion server
Proxies
Proxy server
DMZ Subnet
Application server
Private Subnet
RDS DB
M
Private Subnet
VPC
Dev VPC
Availability zone A
Dev App server
Dev DB
M
Public Subnet
Users
Load balancers
Proxies
Proxy server
DMZ Subnet
Application server
Private Subnet
RDS DB
S
Private Subnet
Availability zone B
Sec. offsite bkup
>1000km range
from Primary
backup
backup
S3 (Private)
Database and
Code backups,
(Encrypted)

2 Data Security

Yellow Schedule has been specifically developed to ensure that access to your data is secure, fast, always available and that hardware systems are fault tolerant, so our customers always trust us with their most sensitive data.

Data Security

Specific security controls ensure that only you have access to your data;

- 256bit SSL (TLS1.2) secures data in transit.
- PHI/PII data encrypted at rest (Rijndael AES256 encryption).
- Backups and data replication secured to non-public data warehouse facilities.
- Controlled access to data.
- Firewall and cloud security groups control access to system hardware.
- Multifactor authentication function is provided which involves text message verification at regular intervals or on any login attempts on
- unrecognised devices.
- AWS Cloudwatch used for log/event management and alerting purposes.
- Internal staff controls for key management and password control.
- Separate secure environments for development, testing, and production
- Our product software and infrastructure is updated regularly with the latest security patches.
- Minimum requirements on password complexity. Also customizable options for password complexity on case-by-case requirements basis. (One
- institution may require passwords to be minimum 16 characters with a mix of lowercase, uppercase, numbers and special characters, a different
- institution may have different minimum requirements such as 10 characters, but with a forced password change every month, and login timeout
- period if an incorrect password attempt happens a certain number of times)
- User password hashing and salting according to best principles.
- Penetration Testing carried out at regular intervals by top-tier data security partner.
- A documented API and System of Webhooks has been developed for interoperability. This can be used to allow trusted partners to perform CRUD operations programmatically instantly in a secure way.

3 Physical Security Controls

All data is hosted in secure datacenters with the world leaders in managed hosting. Physical security controls used in the datacenter include:

- Keycard protocols.
- Biometric scanning protocols.
- Around-the- clock interior and exterior surveillance.
- Access limited to authorized data center personnel, prior clearance and escort required.
- Thorough background security checks on Data center employees.
- Best Environmental controls including:
    - N+1 redundant HVAC (Heating Ventilation Air Conditioning) system
    - Advanced fire suppression systems.
    - Every 90 seconds, all air is circulated and filtered to remove dust and contaminants.

4 Backup Controls

Your data is safe. We take nothing to chance and have numerous processes in place to protect against any potential data loss:

- Secure database replication system ensures lossless replication across multiple availability zones.
- Secure system of data backups.
- Advanced monitoring systems pre-alert staff where any exceptions occur (memory spikes, high CPU usage etc).
- All critical devices reside on dual power supply systems.
- Geographically distributed backups to secure facilities on the opposite side of the continent.
- Backup and restoration processes are regularly tested.
- Optimized databases and load balanced servers ensure you'll never be waiting for your data.
- Audit history allows users to track changes to client data.

5 HIPAA

Yellow Schedule has been specifically developed to ensure that access to your data is secure, fast, always available and that hardware systems are

All US based health care organizations need to be HIPAA compliant. It’s up to each organisation to ensure compliance, there is no such thing as ‘HIPAA Compliant Software’. However software should enable your organisation to fulfil all its obligations in regard to the electronic storage of patient information.

YellowSchedule enables our customers to:

- Track who did what
- Define user roles
- Ensure data security
- Ensure maximum ‘up time’ of the system and availability of a backup

6 GDPR

The General Data Protection Regulation (GDPR) is Europe's framework for data protection laws and is the toughest privacy and security law in the world. As a global solution, we are excited to announce that Yellow Schedule is fully compliant with the GDPR standards for handling user and patient personal data. Yellow Schedule serves thousands of businesses and healthcare bodies globally with best-in-class scheduling, requiring the storing of patient, appointment, and user information within our platform. The success of our solution comes with responsibility to hold ourselves accountable for the privacy and security of the data held within the system. Becoming GDPR compliant on EU based infrastructure strengthens our commitment to provide a secure platform that protects personal information and serves the needs of our users.

7 PHIPA / PIPEDA

Under PHIPA (PIPEDA is declared substantially similar to PIPEDA) Yellow Schedule is considered an electronic service provider. In regards to this our service and system is fully compliant in regards to its use of PHI, secure storage and backup.