# CAPSTONE PROJECT 3 – mediCARE

## IN4.0 GROUP TALENT ACADEMY

David Brown / Georgios Evangelinos / Jonah Froggatt / Romeela Nawaz / Jordan Wheeler

## Introduction

The following report discusses the development of an Amazon Web Services (AWS) architecture for MediCARE, a private health company based in Blackpool that intends to kickstart a flu vaccination programme. The objectives are the migration of their existing on-prem patients' database to the cloud and the design of a cloud infrastructure that will host the database and alert all patients with a pre-existing lung condition to book an appointment for the vaccination programme via SMS and email. The proposed architecture was based on the principles of the AWS' Well-Architected Framework (WAF)[28] and Cloud Adoption Framework (CAF)[29], aiming to achieve maximum functionality, in addition to high reliability and availability, with optimised costs.

## Architected Solution Methodology

AWS Database Migration Service will be used to securely upload the on-premises database to the RDS instance contained within a private subnet inside the VPC[33]. It allows the on-premises server to be live while it migrates, minimising downtime and allowing MediCARE to fully operate[32]. Depending on the data model, a scheme conversion tool may be required. The client would only pay for the compute resources used during the migration process and any additional log storage which means its a low cost service. The AWS DMS will ensure accurate and secure transit by monitoring the source and target databases.

Using Amazon Aurora with an RDS instance will allow us to automate processes such as hardware provisioning, database setup, scaling, and backups[35], increasing operational efficiency[28]. The data will be encrypted at rest and in transit to further increase security[28]. A SQL database is recommended to allow for report building capability. AWS RDS will work in tandem with AWS Lambda to automate encrypted backups to the on-premises server on a daily basis[35], which is a key requirement from MediCARE.

Regarding security, MediCARE will use a well-defined VPN that protects traffic in and out of the resources, while utilising the flow logs to monitor the traffic within the network. They will also configure the security group and the Network access control list to act as a firewall.

Initial costs:

Based on the size of the database ((100*150000)*12)/1024/1024/1024= 0.167 GB.

A db.t2. small instance would be initially provisioned with Aurora MySQL at £25.73 per month. This can be scaled as required.

## Form Building

For the form creation requirement, a serverless model using step functions was used in order to increase performance efficiency[28]. It will orchestrate the S3, Route53 and CloudFront services to allow a one-time, pre-signed URL [10][16] to be sent to the desired patients, this will then be monitored by CloudWatch[17] that will monitor which links have been followed and store that data in an RDS database to allow automated report building for the MediCARE staff.

Figure 1 shows how this has been achieved, by creating a user-friendly front-end API interface, which will require the staff to log in (using MFA). It will be a simple web application that will connect to an API, allowing the creation of forms[A2]. An API request will be sent to the cloud using an encrypted JSON stream, this will be the only stream in this area of the architecture that will be outside of the cloud, and once the data is inside the cloud, it is then secured by AWS. This POST request will trigger the first set of step functions, which will create a new table in the Form database, followed by another lambda which will take the stored HTML skeleton and add the required fields, then add it to an S3 bucket.

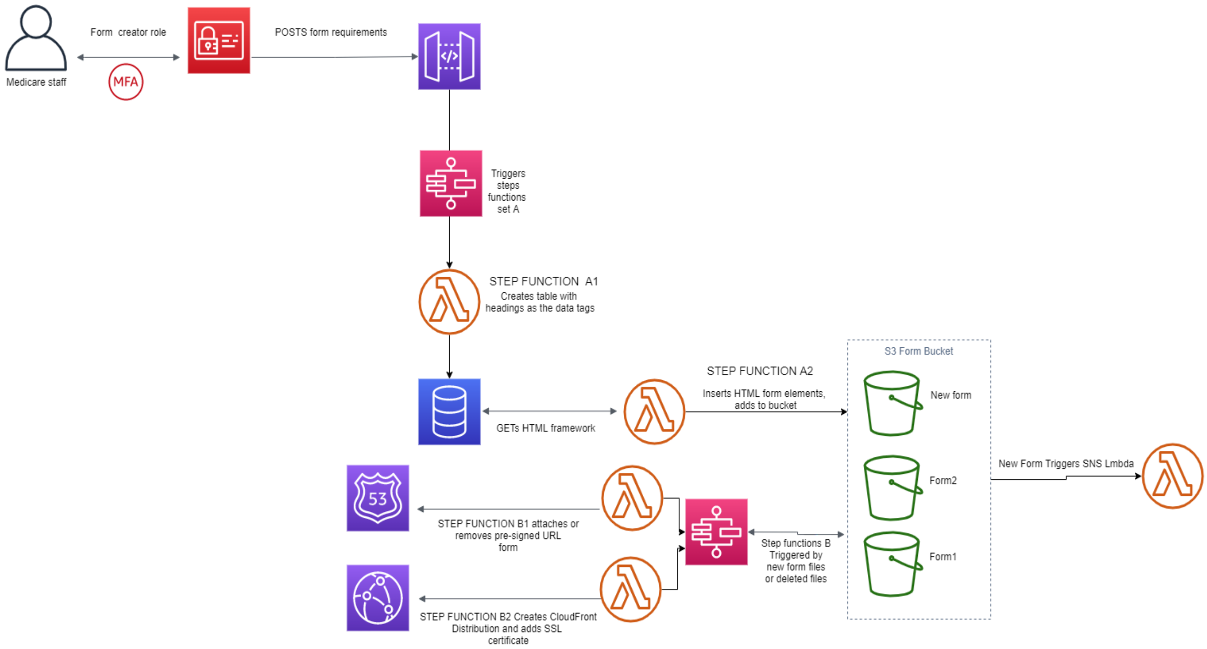
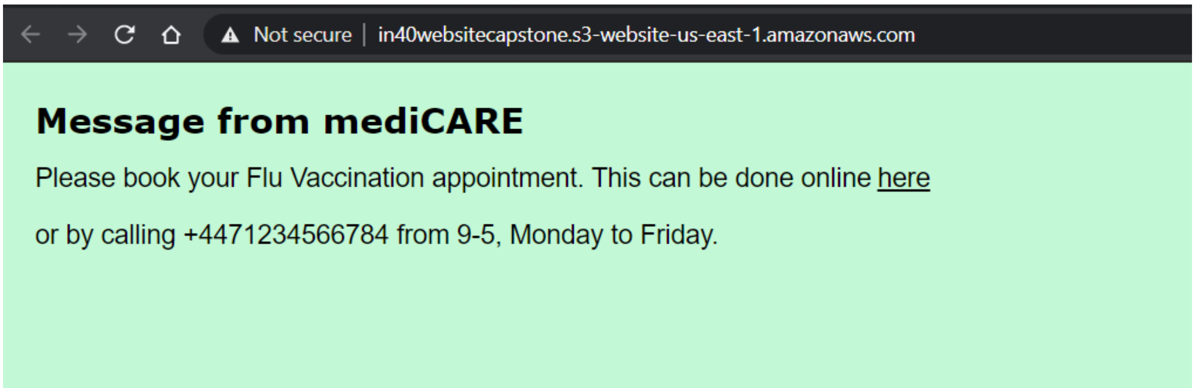

Medicare staff
Form creator role
MFA
POSTS form requirements
Triggers steps functions set A
STEP FUNCTION A1
Creates table with headings as the data tags
STEP FUNCTION A2
Inserts HTML form elements, adds to bucket
GETs HTML framework
S3 Form Bucket
New form
Form2
Form1
New Form Triggers SNS Lmbda
53
STEP FUNCTION B1 attaches or removes pre-signed URL form
Step functions B Triggered by new form files or deleted files
STEP FUNCTION B2 Creates CloudFront Distribution and adds SSL certificate

Figure 1: Form creation architecture

To make the forms available to the right patients, and to keep inline with GDPR[18], another set of step functions are triggered which will create a CloudFront distribution[13] along with it's SSL certificate, and assign a one-time, pre-signed URL[10][16] to the form and store this data in the PatientContacts database in order to trigger the notification Lambdas. To track user-interaction CloudWatch will monitor traffic to the distribution logging which links have been followed, in order to generate weekly reports for the MediCARE staff.

As mediCARE doesn’t have to pay for uptime of the underlying infrastructure, they only have to pay the costs that are required for when the service is used, this service is practically free. For example, 500 forms being created with every patient filling out at least one form would result in a cost of around £1 per month.

## Push Notifications, Report Building & Logging



Not secure | in40websitecapstone.s3-website-us-east-1.amazonaws.com

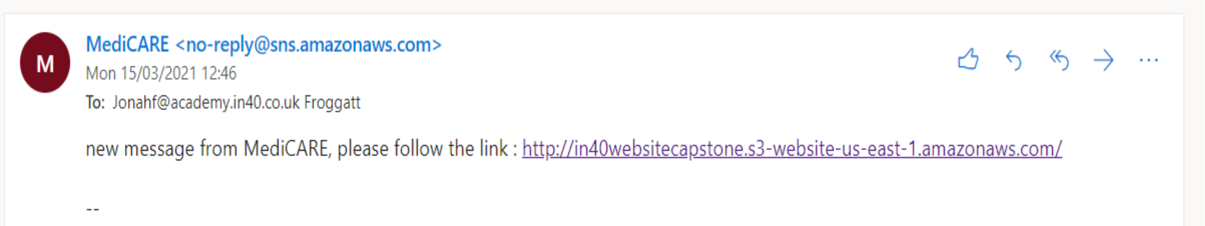
**Message from mediCARE**

Please book your Flu Vaccination appointment. This can be done online here

or by calling +4471234566784 from 9-5, Monday to Friday.

Figure 2: Example web message

In terms of email/SMS delivery, there are only a few options. Both email and SMS messages are to be delivered using Amazon Simple Notification Service (SNS), which would both contain a link to an S3 static website with a message telling the patient to book an appointment, with the necessary details to do so. Each link would be unique per patient and would be sent to both their phone and email. The links would then be monitored using Amazon CloudWatch. [23] Using SES was considered for the email, but in terms of simplicity it makes sense to do both through SNS. [24] Also, as the message is hosted on a static website, MediCARE don’t need the extra functionality, furthermore, emails through SNS are cheaper than in SES, adhering to the cost optimisation pillar of the CAF[25][26]. Each individual link is set to expire after one click, increasing the security of the message, which adheres to the Security pillar[28].

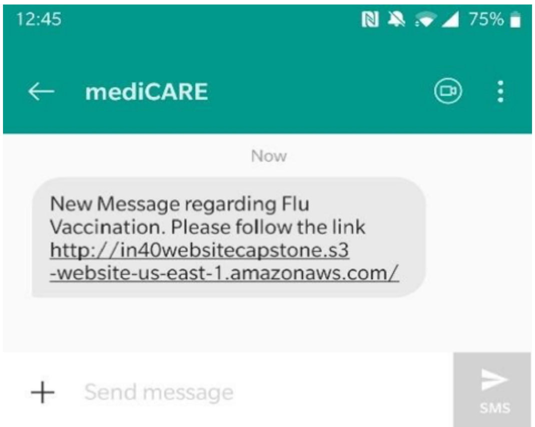


MediCARE <no-reply@sns.amazonaws.com>
Mon 15/03/2021 12:46
To: Jonahf@academy.in40.co.uk Froggatt

new message from MediCARE, please follow the link : http://in40websitecapstone.s3-website-us-east-1.amazonaws.com/

--

Figure 3: Email example



New Message regarding Flu Vaccination. Please follow the link http://in40websitecapstone.s3-website-us-east-1.amazonaws.com/

Figure 4: Example of SMS message

In terms of pricing, to send one message to every patient with a lung condition (roughly 112,500 patients), it would cost about £3100. This is similar across all the AWS text messaging services [27], and as this is required, this is a necessary cost. The emails would only cost about £2 for the same number of messages[25][26], and push notifications are similarly cheap, so it may be worth mediCARE considering taking that option instead.

Following the creation of email/SMS notifications, the architecture should cater for generating reports and logging that would indicate whether each individual patient has interacted with his unique vaccination registration link. Thus, MediCARE could easily create a separate set of records with all the unregistered patients and send them weekly reminders to register for the vaccination programme.

In order to avoid the addition of redundant services and unnecessary additional costs to the architecture, the services of Amazon SNS and Amazon Cloudwatch from the previous phase could be used further. To begin with, Amazon Cloudwatch would be responsible for monitoring the individual links and triggering a Lambda function (Λ1), whenever a personalised link is followed and store the respective patient's record in a database table (under the name "Respondents"). Another Lambda (Λ2) will be implemented and set to trigger on a weekly basis, to retrieve data from both the Patient & Respondents DB tables and, by comparison, filtering the non-respondents. The non-respondents' records will be stored in a third database table and a weekly report in human-readable format could be generated [30]. A third Lambda function (Λ3) will be used to read through the non-respondents DB table and repeat the process by triggering the SNS service.

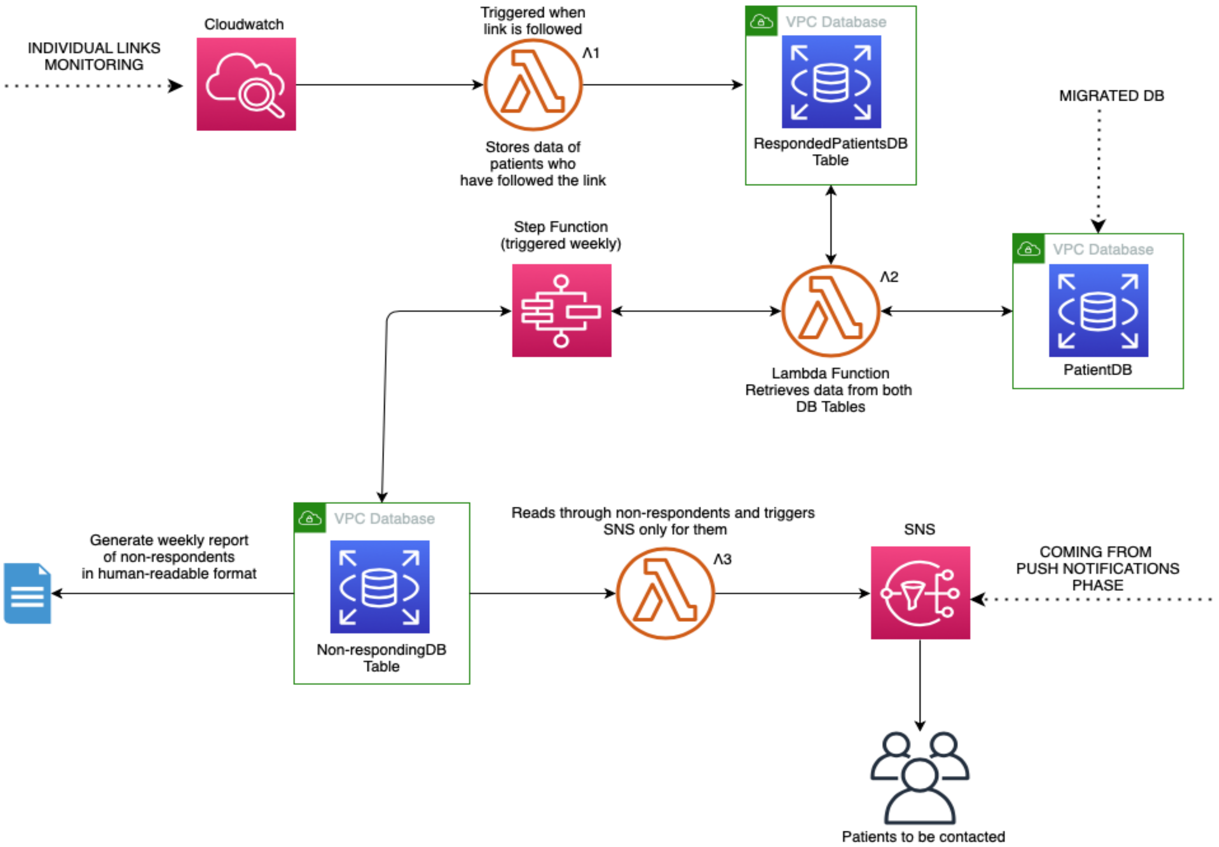

INDIVIDUAL LINKS MONITORING
Cloudwatch
Triggered when link is followed
Λ1
Stores data of patients who have followed the link
VPC Database
RespondedPatientsDB Table
MIGRATED DB
Step Function (triggered weekly)
Λ2
Lambda Function Retrieves data from both DB Tables
VPC Database
PatientDB
VPC Database
Non-respondingDB Table
Generate weekly report of non-respondents in human-readable format
Reads through non-respondents and triggers SNS only for them
Λ3
SNS
COMING FROM PUSH NOTIFICATIONS PHASE
Patients to be contacted

Figure 5: monitoring and report building architecture

This architecture is simplistic and comes with three major advantages:

- Utilising existing architecture,
- Avoiding the addition of extra and potentially redundant services (such as SSRS, AWS SES)[31][24].
- Keeping costs at a minimum.

## Security & Cost Optimisation

The responsibility of security and compliance is shared between AWS and the customer, which means AWS takes care of the underlying cloud infrastructure and MediCARE is responsible for securing the workload that is deployed in AWS[20]. This shared model helps to relieve the customer's burden (see figure 6).

Data security is a vital part for MediCARE as they hold confidential patient information. It was ensured that the security principle from the CAF and WAF were followed. Amazon Virtual Private Cloud (Amazon VPC) is a service that is used to build a custom-defined network in the AWS Cloud. It is recommended to create multiple VPCs to separate networking environments and ensure confidential data remains secure.

Two key services which are implemented to improve security are AWS Identity and Access Management (IAM) and Multi Factor Authentication (MFA). With IAM, multiple users can be created from a single AWS account and the staff can be given individual security credentials. MFA provides an extra level of security and when enabled, the users will be prompted to enter their username and password along with an authentication code sent to their chosen device to confirm their identity. This prevents unauthorised access to the AWS environment and secures the data.

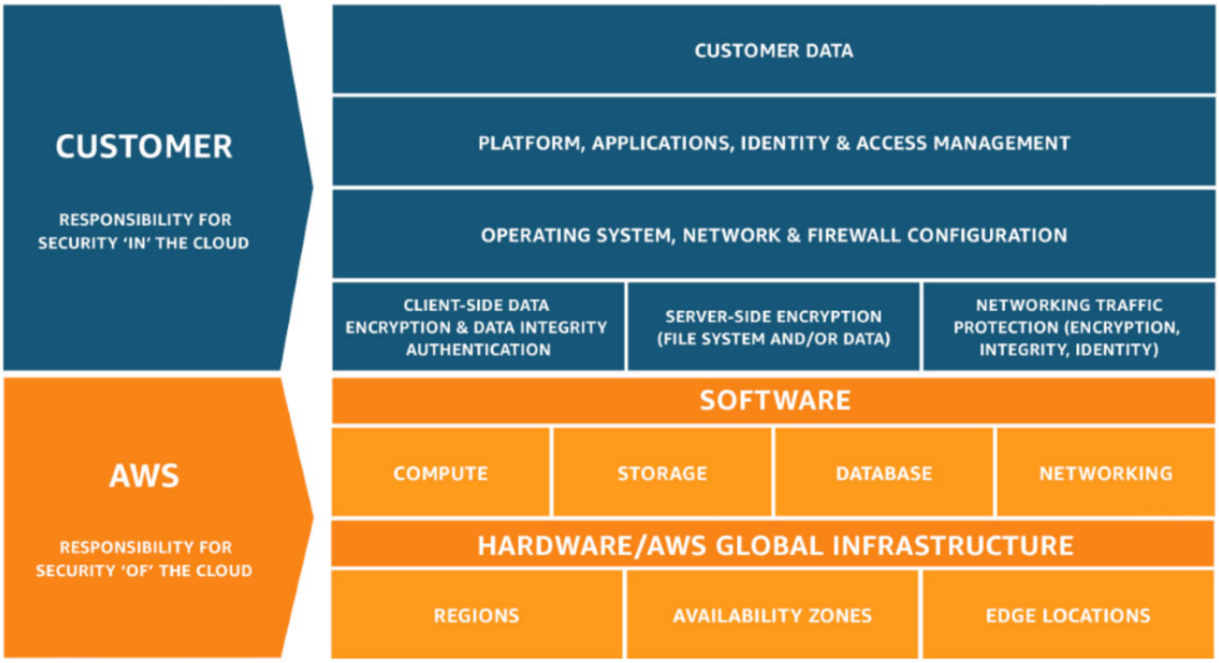

CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Figure 6: The security of the cloud is AWS's responsibility whereas the security in the cloud is the customers.

CloudTrail Instances are used to log and monitor account activity. CloudTrail provides event history which can be used by MediCARE to continuously monitor the databases.

Amazon's Trusted Advisor[22] checks will optimize MediCARE's AWS infrastructure by identifying security misconfigurations as well as providing suggestions for improving system performance. It also informs of underutilised resources which will reduce costs.

## Conclusion

This solution is based on the five pillars of the WAF and the six perspectives of the CAF enabling a cohesive, available and resilient architecture. The key points and concerns for MEDIcare were identified and automated, wherever possible, by using the most up-to-date technological advances in order to keep cost and maintenance at a minimum without compromising security due to the sensitivity of the data. There are multiple components and services implemented within the structure: such as Aurora, serverless components, SNS & Cloudwatch. These services are managed by AWS, the mediCARE staff will not have to deal with processes, including responsibility for maintenance, logging and reporting as well as auto-scalability according to demand.

The total cost of this system is approximately £20-£30/month. Non-recurring costs are dominated by the SMS messaging and for each programme they want to begin, mediCARE can expect to spend £3,000-£4,000. For less vital initiatives, mediCARE could consider using email services only, bringing this cost down to £2.

## References:

[1] aws.amazon.com, "Amazon RDS Pricing," [Online]. Available: Amazon RDS Pricing: https://aws.amazon.com/rds/pricing/. [Accessed 2021].

[2] aws.amazon.com, "AWS Lake Formation," [Online]. Available: https://aws.amazon.com/lake-formation/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc.

[3] aws.amazon.com, "Analytics on AWS," [Online]. Available: Analytics on AWS: https://aws.amazon.com/big-data/datalakes-and-analytics/. [Accessed 2021].

[4] docs.aws.amazon.com, "Create Custom Reports and Analyze AppStream 2.0 Usage Data," [Online]. Available: https://docs.aws.amazon.com/appstream2/latest/developerguide/configure-custom-reports-analyze-usage-data.html. [Accessed 2021].

[5] docs.aws.amazon.com, "Create an Analysis Using Your Own Database Data," [Online]. Available: https://docs.aws.amazon.com/quicksight/latest/user/getting-started-create-analysis-database.html. [Accessed 2021].

[6] aws.amazon.com, "Scai - Business Intelligence, Reporting & Analytics for Redshift, RDS," [Online]. Available: https://aws.amazon.com/marketplace/pp/ScaiData-Scai-Business-Intelligence-Reporting-Anal/B07JR92TFG. [Accessed 2021].

[7] www.concurrencylabs.com/blog, "Save yourself a lot of pain (and money) by choosing your AWS Region wisely," [Online]. Available: https://www.concurrencylabs.com/blog/choose-your-aws-region-wisely/. [Accessed 2021].

[8] www.datadoghq.com, "AWS Dashboards / Datadog," [Online]. Available: https://www.datadoghq.com/dg/monitor/aws-dashboards-benefits/?utm_source=Advertisement&utm_medium=GoogleAdsNon1stTier&utm_campaign=GoogleAdsNon1stTier-AWSNonENES&utm_content=AWS&utm_keyword=%2Baws%20%2Breporting&utm_matchtype=b&g. [Accessed 2021].

[9] www.datadoghq.com, "Pricing / Datadog," [Online]. Available: Pricing / Datadog: https://www.datadoghq.com/pricing/.

[10] docs.aws.amazon.com, "Pre-signed URL," [Online]. Available: https://docs.aws.amazon.com/AmazonS3/latest/userguide/ShareObjectPreSignedURL.html. [Accessed 2021].

[11] aws.amazon.com, "Lambda Pricing," [Online]. Available: https://aws.amazon.com/lambda/pricing/.

[12] aws.amazon.com, "Step Function pricing," [Online]. Available: https://aws.amazon.com/step-functions/pricing/. [Accessed 2021].

[13] boto3.amazonaws.com, "CloudFront Lambda integration," [Online]. Available: https://boto3.amazonaws.com/v1/documentation/api/latest/reference/services/cloudfront.html. [Accessed 2021].

[14] aws.amazon.com, "Cloudfront Pricing," [Online]. Available: https://aws.amazon.com/cloudfront/.

[15] docs.aws.amazon.com, "Cloudfront Pricing," [Online]. Available: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/CloudFrontPricing.html. [Accessed 2021].

[16] boto3.amazonaws.com, "Route53 Lambda integration," [Online]. Available: https://boto3.amazonaws.com/v1/documentation/api/latest/reference/services/route53.html#Route53.Client.generate_presigned_url . [Accessed 2021].

[17] www.serverless.com, "One-time Pre-signed URL using serverless model," [Online]. Available: https://www.serverless.com/blog/s3-one-time-signed-url. [Accessed 2021].

[18] aws.amazon.com, "CloudWatch," [Online]. Available: https://aws.amazon.com/cloudwatch/.

[19] gdpr-info.eu, "GDPR Document," [Online]. Available: https://gdpr-info.eu/ . [Accessed 2021].

[20] aws.amazon.com, "AWS Shared Responsibility Model," [Online]. Available: https://aws.amazon.com/compliance/shared-responsibility-model/ . [Accessed 2021].

[21] docs.aws.amazon.com, "AWS Security," [Online]. Available: https://aws.amazon.com/Security/ . [Accessed 2021].

[22] aws.amazon.com, "AWS Cost optimisation/ Trusted Advisor," [Online]. Available: https://aws.amazon.com/aws-cost-management/aws-cost-optimization/ . [Accessed 2021].

[23] docs.aws.amazon.com, "Monitoring S3 requests with cloudwatch:," [Online]. Available: https://docs.aws.amazon.com/AmazonS3/latest/userguide/cloudtrail-request-identification.html. [Accessed 2021].

[24] stackshare.io, "SES vs SNS," [Online]. Available: https://stackshare.io/stackups/amazon-ses-vs-amazon-sns. [Accessed 2021].

[25] aws.amazon.com, "SES Pricing," [Online]. Available: https://aws.amazon.com/ses/pricing. [Accessed 2021].

[26] aws.amazon.com, "SNS Pricing," [Online]. Available: https://aws.amazon.com/sns/pricing. [Accessed 2021].

[27] aws.amazon.com, "Pinpoint Pricing for text price comparison," [Online]. Available: https://aws.amazon.com/pinpoint/pricing/.

[28] docs.aws.amazon.com, "WAF whitepaper," [Online]. Available: https://docs.aws.amazon.com/wellarchitected/latest/framework/wellarchitected-framework.pdf. [Accessed 2021].

[29] d1.awsstatic.com, "CAF whitepaper," [Online]. Available: https://d1.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf. [Accessed 2021].

[30] devart.com, "Data Export from Amazon RDS Instance," [Online]. Available: https://blog.devart.com/data-export-from-amazon-rds-mysql-instance.html. [Accessed 14 3 2021].

[31] M. E., "SSRS Reporting Basics: When is SSRS the Right Tool?," [Online]. Available: https://www.red-gate.com/simple-talk/sql/bi/ssrs-reporting-basics-when-is-ssrs-the-right-tool/.

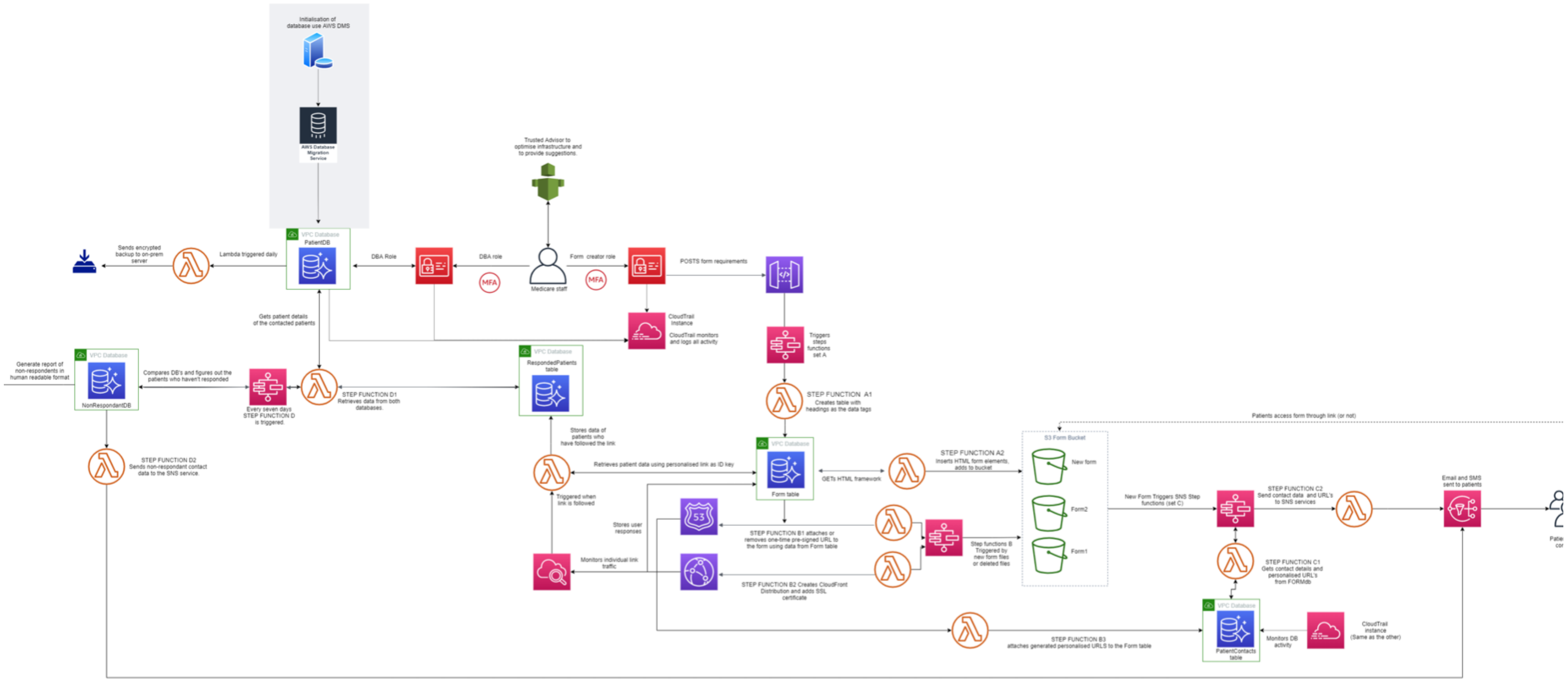
[32] aws.amazon.com, "AWS DMS," [Online]. Available: https://aws.amazon.com/dms/. [Accessed 2021].

[33] A. r. (vitalsource.com), "AWS Virtual Private Cloud," [Online]. Available: AWS re/Start (vitalsource.com). [Accessed 2021].

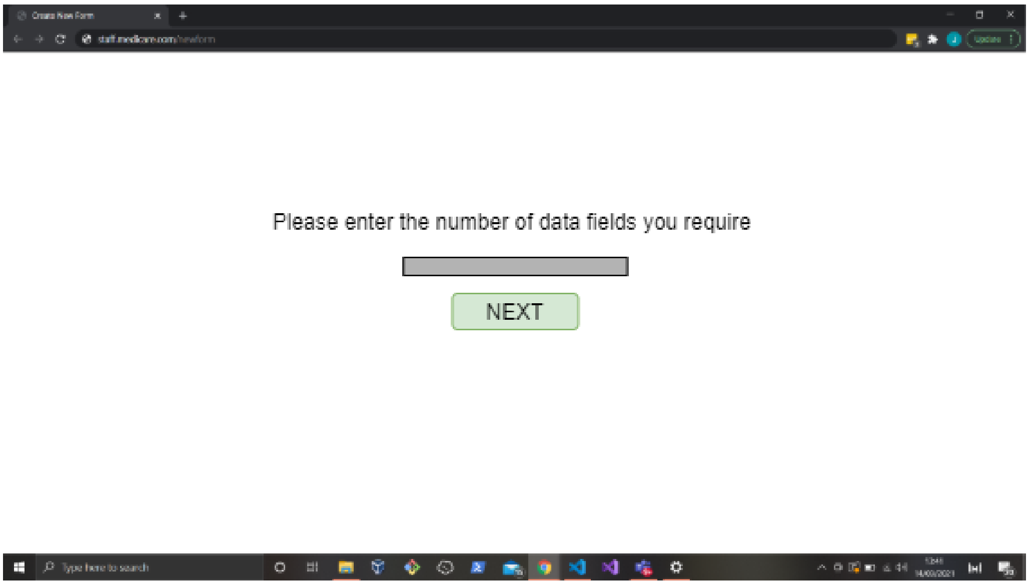
[34] A. D. M. S. -. A. W. Services, "AWS Database Migration Service," [Online]. Available: https://aws.amazon.com/dms/?did=ft_card&trk=ft_card. [Accessed 2021].

[35] aws.amazon.com, "Amazon RDS," [Online]. Available: https://aws.amazon.com/rds/?did=ft_card&trk=ft_card. [Accessed 2021].

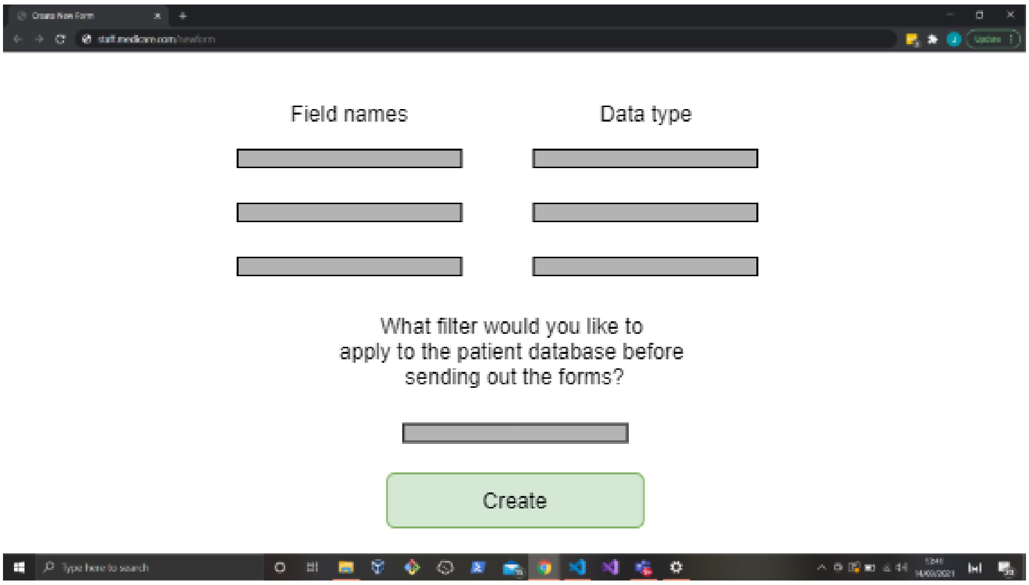
A1.


Initialisation of database use AWS DMS
AWS Database Migration Service
Trusted Advisor to optimise infrastructure and to provide suggestions.
Sends encrypted backup to on-prem server
Lambda triggered daily
VPC Database
PatientDB
DBA Role
DBA role
MFA
Medicare staff
Form creator role
MFA
POSTS form requirements
CloudTrail Instance
CloudTrail monitors and logs all activity
Gets patient details of the contacted patients
Triggers steps functions set A
STEP FUNCTION A1
Creates table with headings as the data tags
Generate report of non-respondents in human readable format
VPC Database
NonRespondantDB
Compares DB's and figures out the patients who haven't responded
Every seven days STEP FUNCTION D is triggered.
STEP FUNCTION D1
Retrieves data from both databases.
VPC Database
RespondedPatients table
STEP FUNCTION D2
Sends non-respondant contact data to the SNS service.
Stores data of patients who have followed the link
Retrieves patient data using personalised link as ID key
Triggered when link is followed
VPC Database
Form table
GETs HTML framework
STEP FUNCTION A2
Inserts HTML form elements, adds to bucket
Patients access form through link (or not)
S3 Form Bucket
New form
Form2
Form1
Stores user responses
STEP FUNCTION B1 attaches or removes one-time pre-signed URL to the form using data from Form table
Step functions B Triggered by new form files or deleted files
Monitors individual link traffic
STEP FUNCTION B2 Creates CloudFront Distribution and adds SSL certificate
New Form Triggers SNS Step functions (set C)
STEP FUNCTION C2
Send contact data and URL's to SNS services
Email and SMS sent to patients
Patie
co
STEP FUNCTION C1
Gets contact details and personalised URL's from FORMdb
STEP FUNCTION B3
attaches generated personalised URLS to the Form table
VPC Database
PatientContacts table
Monitors DB activity
CloudTrail instance (Same as the other)

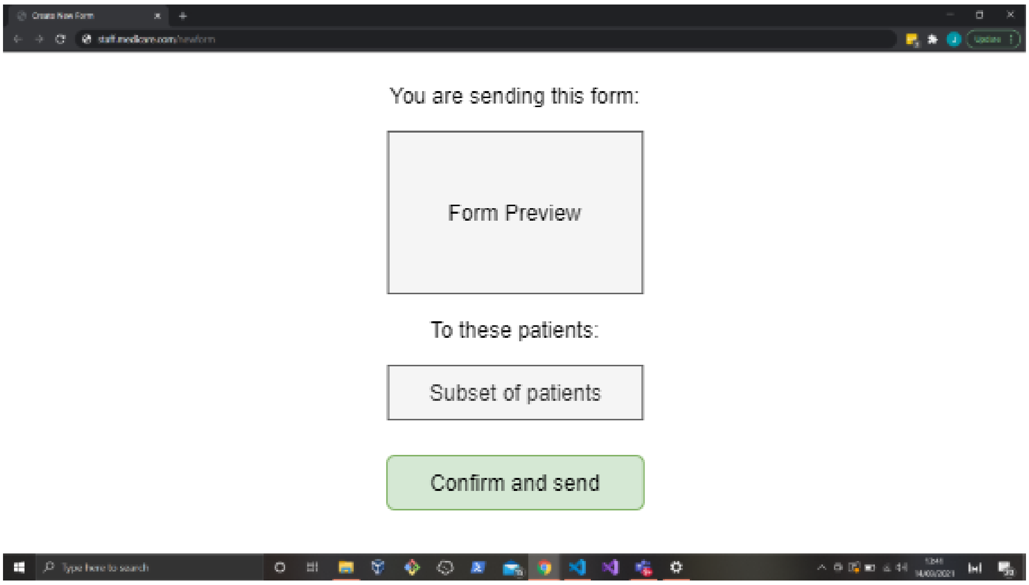
A2.



Please enter the number of data fields you require



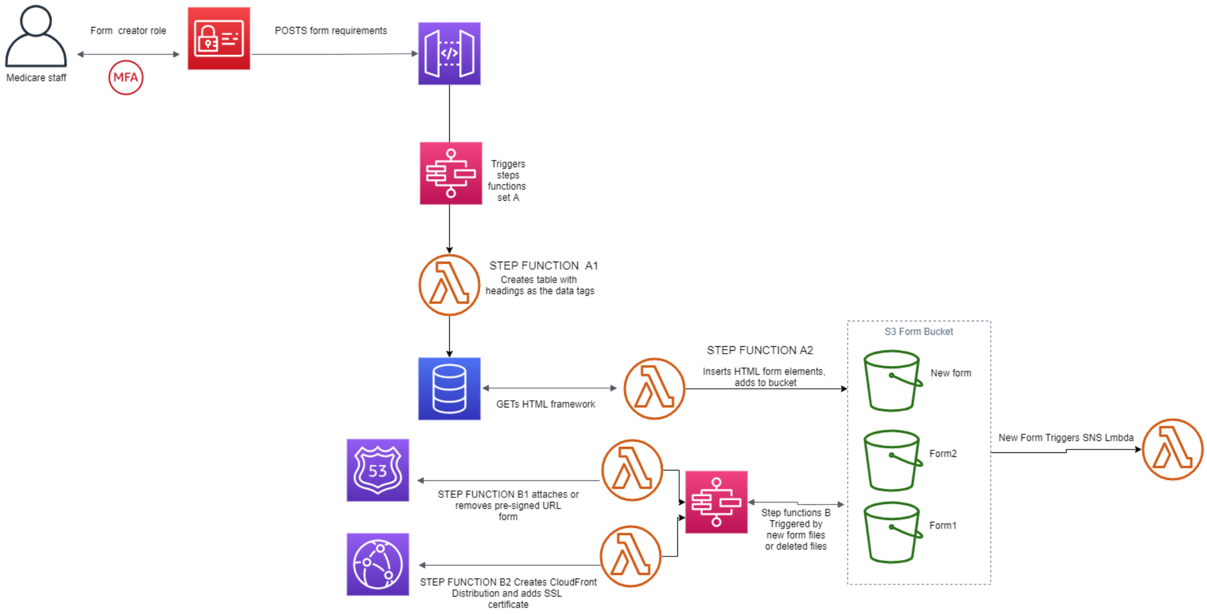
What filter would you like to apply to the patient database before sending out the forms?



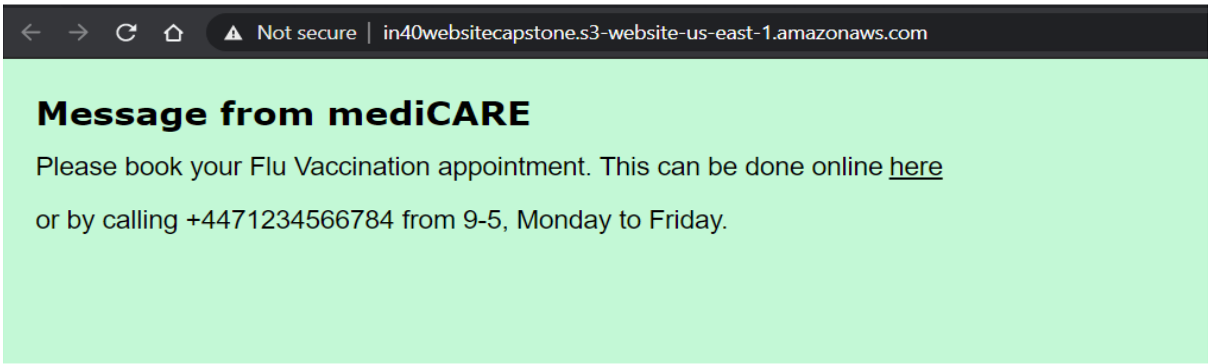
You are sending this form:

To these patients:

A3.


Medicare staff
Form creator role
MFA
POSTS form requirements
Triggers steps functions set A
STEP FUNCTION A1
Creates table with headings as the data tags
GETs HTML framework
STEP FUNCTION A2
Inserts HTML form elements, adds to bucket
S3 Form Bucket
New form
Form2
Form1
New Form Triggers SNS Lmbda
53
STEP FUNCTION B1 attaches or removes pre-signed URL form
Step functions B Triggered by new form files or deleted files
STEP FUNCTION B2 Creates CloudFront Distribution and adds SSL certificate

A4.

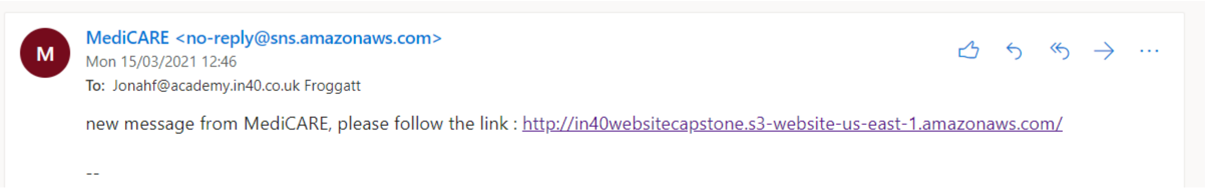

Not secure | in40websitecapstone.s3-website-us-east-1.amazonaws.com

## Message from mediCARE

Please book your Flu Vaccination appointment. This can be done online here

or by calling +4471234566784 from 9-5, Monday to Friday.

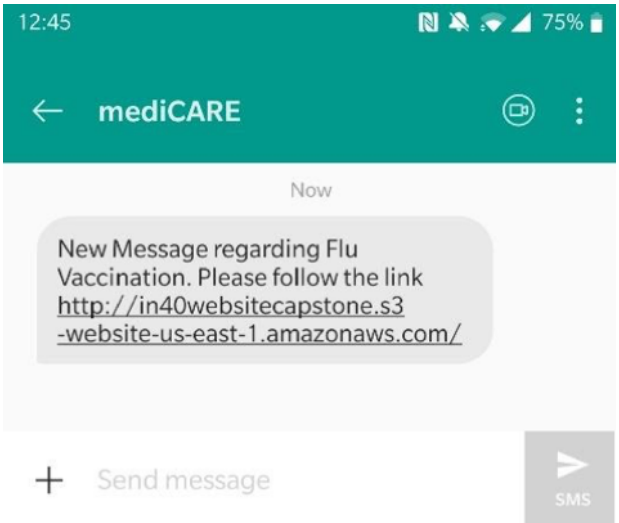
A5.


MediCARE <no-reply@sns.amazonaws.com>
Mon 15/03/2021 12:46
To: Jonahf@academy.in40.co.uk Froggatt

new message from MediCARE, please follow the link : http://in40websitecapstone.s3-website-us-east-1.amazonaws.com/

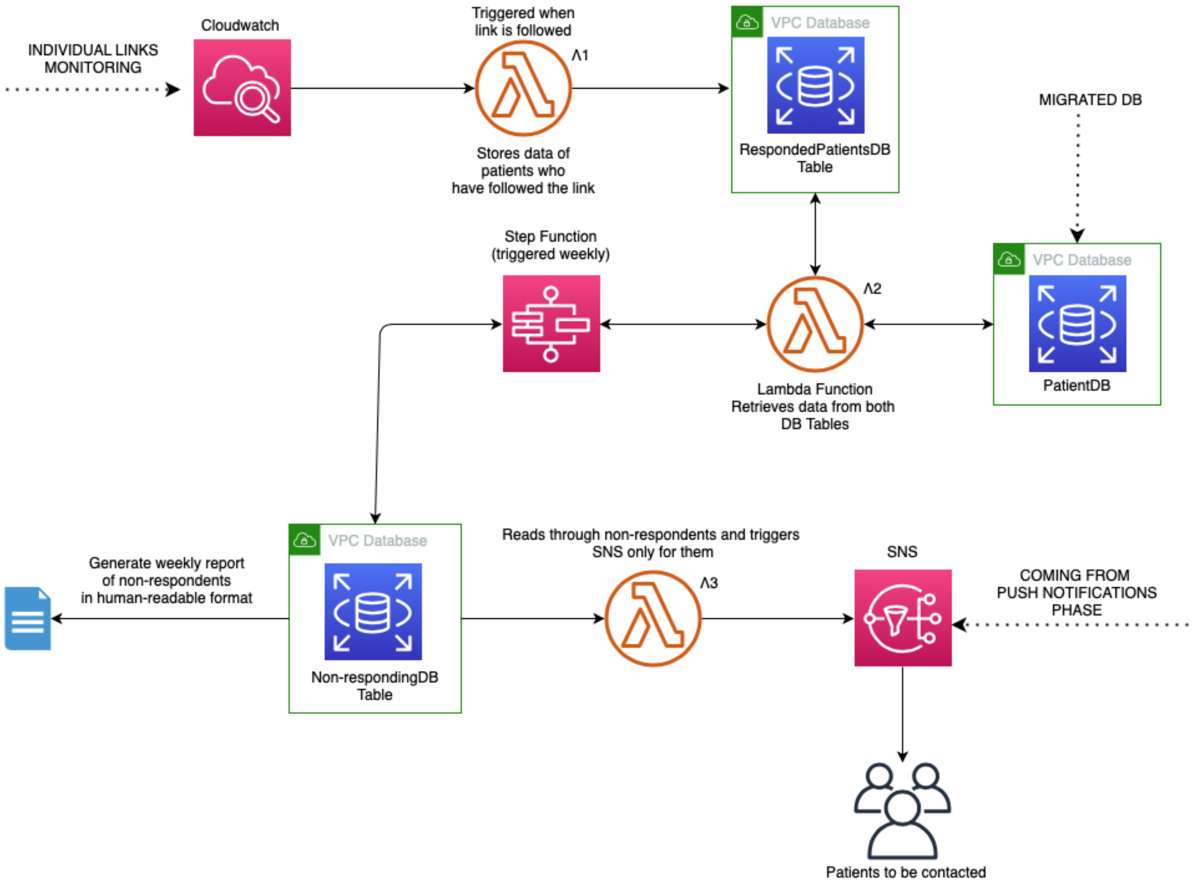
--

A6.



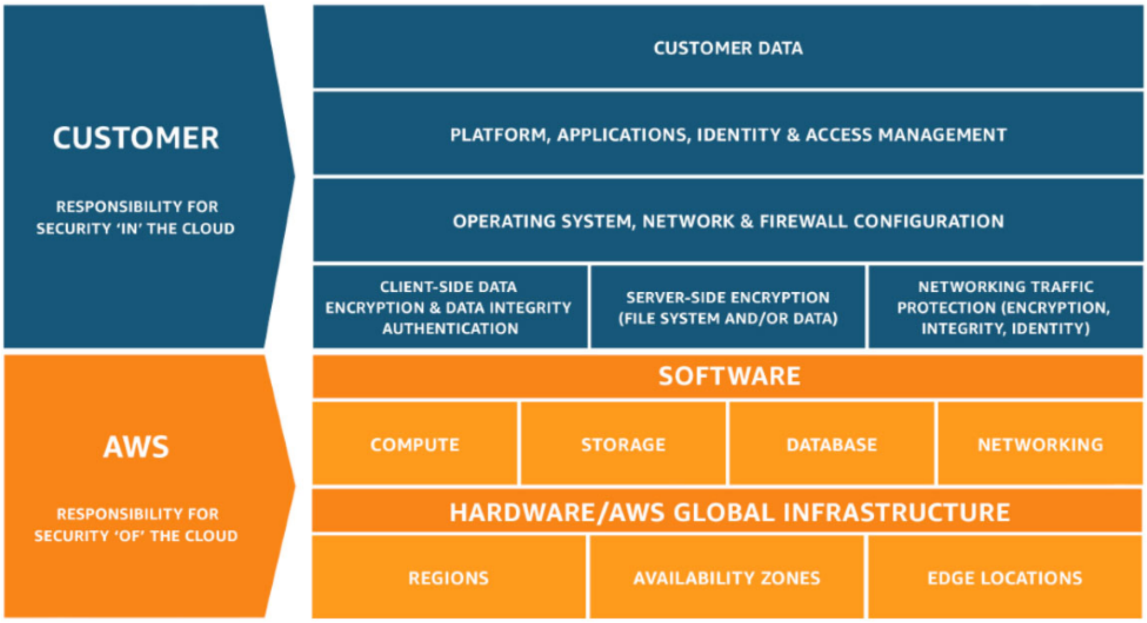
New Message regarding Flu Vaccination. Please follow the link http://in40websitecapstone.s3-website-us-east-1.amazonaws.com/

A7.



INDIVIDUAL LINKS MONITORING
Cloudwatch
Triggered when link is followed
Λ1
Stores data of patients who have followed the link
VPC Database
RespondedPatientsDB Table
MIGRATED DB
Step Function (triggered weekly)
Λ2
Lambda Function Retrieves data from both DB Tables
VPC Database
PatientDB
VPC Database
Non-respondingDB Table
Generate weekly report of non-respondents in human-readable format
Reads through non-respondents and triggers SNS only for them
Λ3
SNS
COMING FROM PUSH NOTIFICATIONS PHASE
Patients to be contacted

A8.



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

A9.

KEY

RDS

Lambda Function

MFA Multi Factor Authentication

API Gateway

S3 Bucket

Simple Notification Service

53 Route 53

Step Functions

CloudFront

Identity and Access Management

CloudWatch

CloudTrail