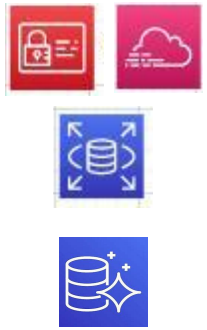
Capstone Project 3 – Architecture Solution

Medicare, a private health company based in Blackpool, has kickstarted a flu vaccination programme. As part of this programme, they aim to alert all patients with a pre-existing lung condition that they need to book a flu vaccination.



Their patient database has 150,000 records and they estimate 25% of them will not have a pre-existing lung condition. All data is currently stored in their on-prem server.

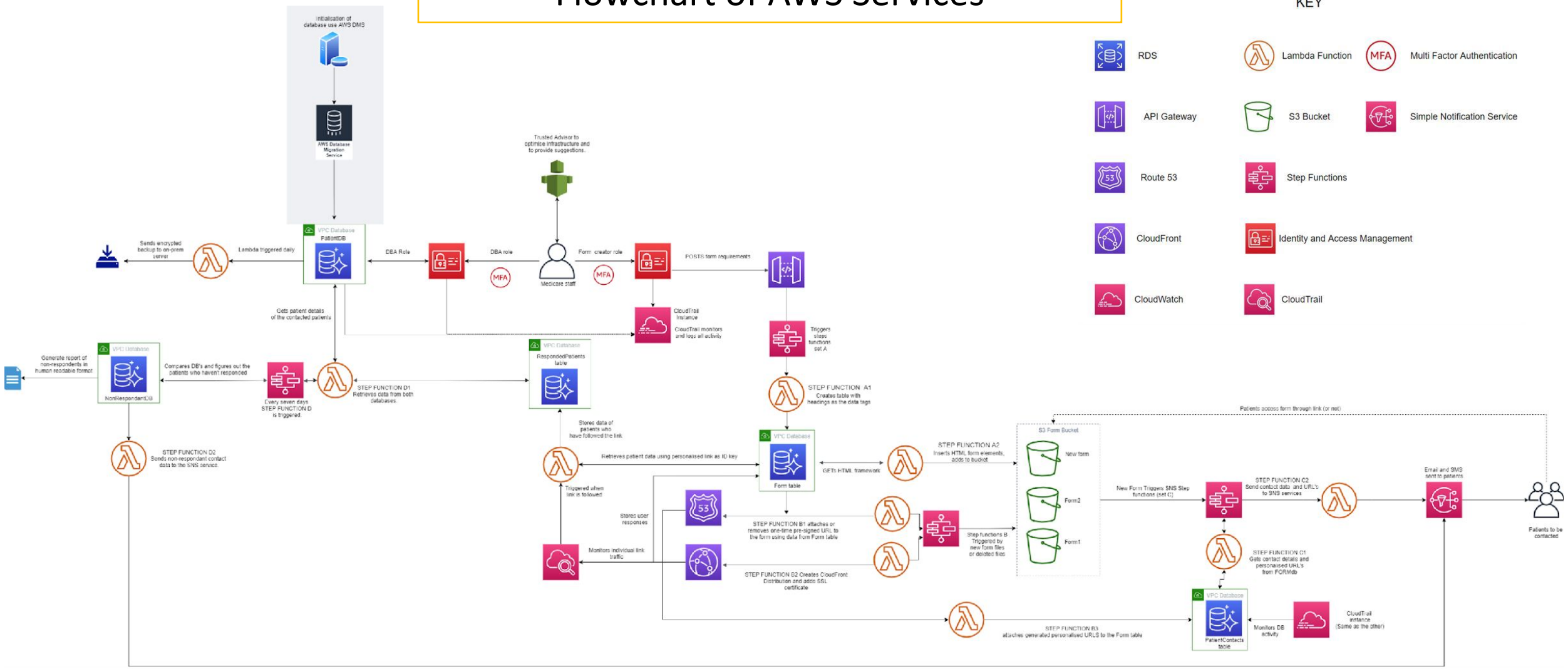
Architect a solution that would allow the company to securely upload their patient database, select all patients who have a pre-existing lung condition, and send an email and a SMS notification to each patient with a link to an online message asking them to book an appointment.

The admin staff must receive a report on patients who have not acknowledged the initial message on a weekly basis.

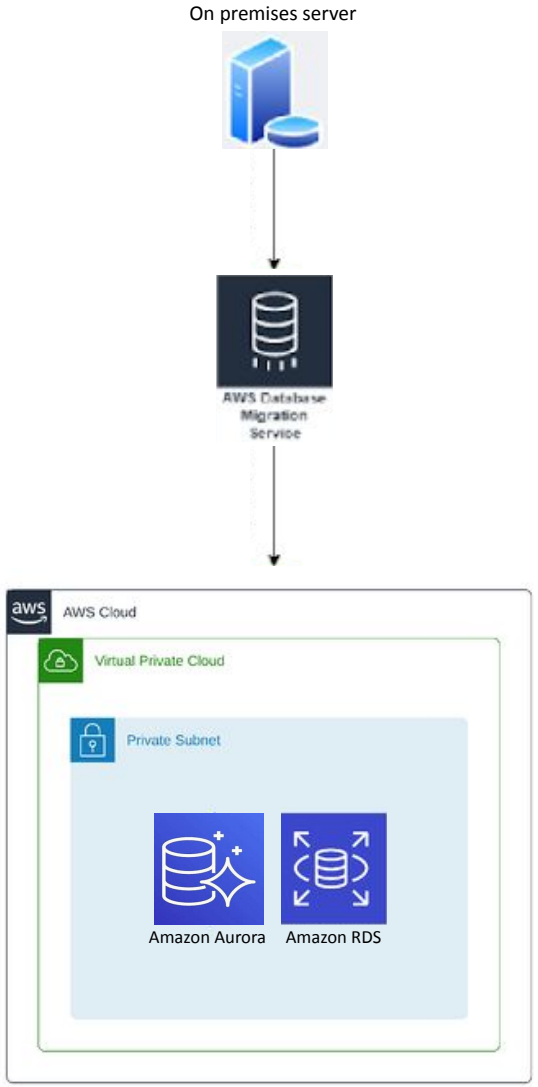
Create a database that shows a list of patients that have followed the link. The architecture must allow for creating forms, adding different kinds of forms, and for retrieving and creating reports as required.

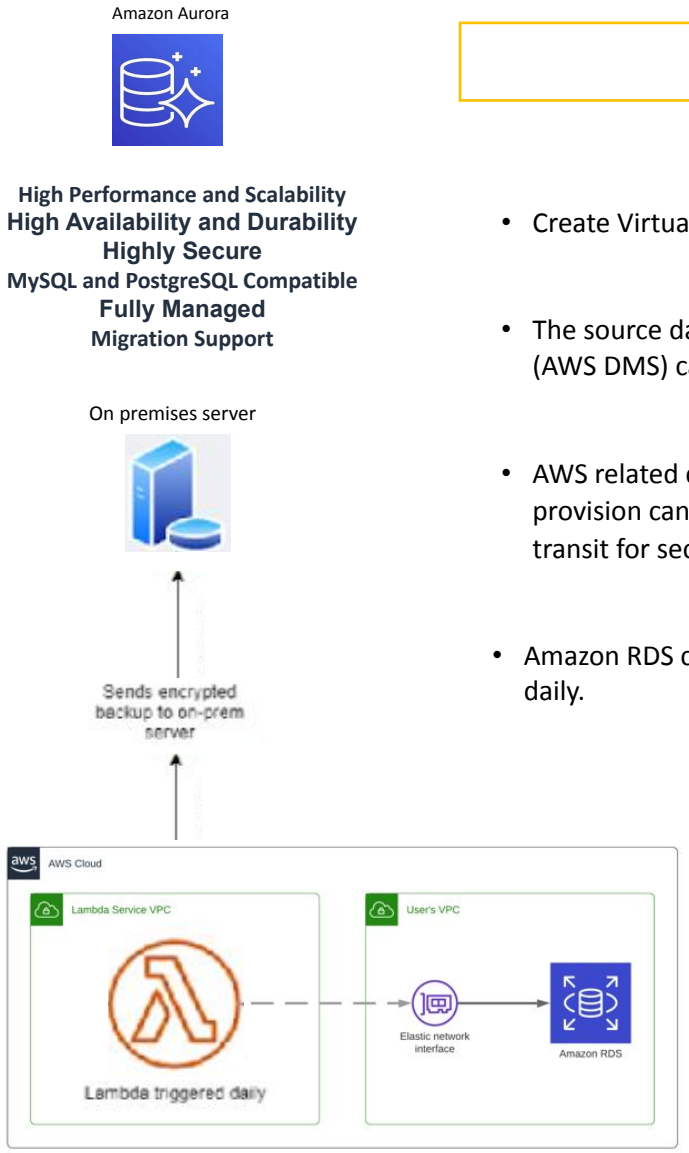
Because of the sensitivity of the data, a backup must be encrypted stored in-house every day.

Flowchart of AWS Services



VPC, DMS, RDS, Amazon Aurora

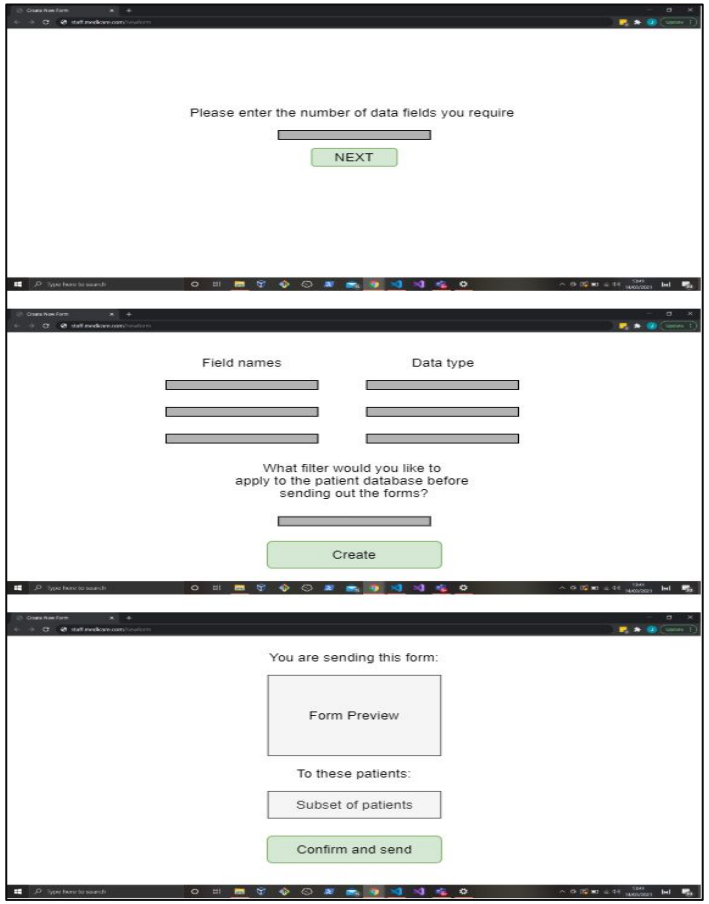




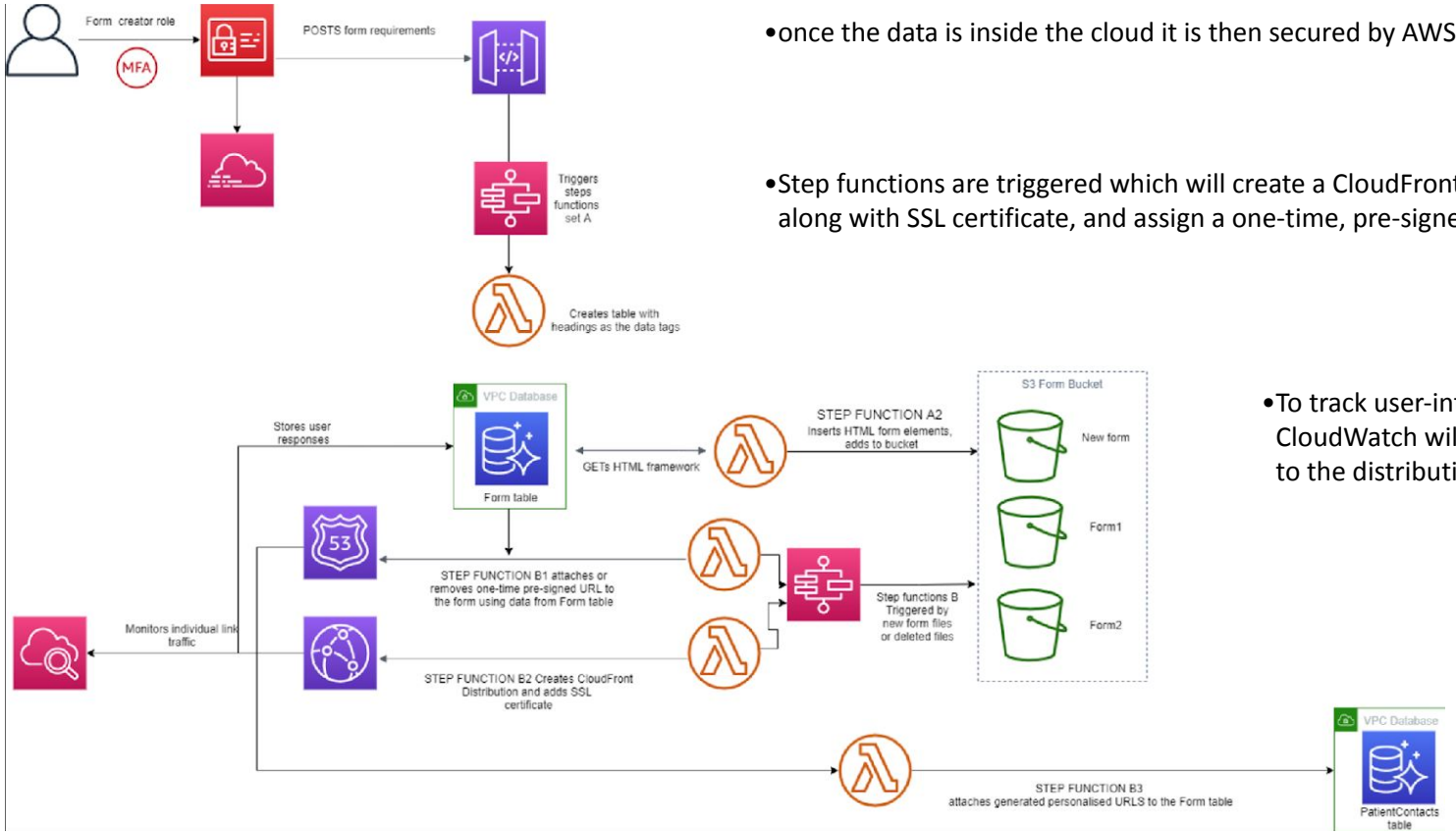
- Create Virtual Private Cloud (VPC) for database instance with AWS VPC
- The source database is located on premises outside of AWS, AWS Database migration service (AWS DMS) can be used to securely upload data to our RDS instance in the VPC
- AWS related database services are easy to use and have best practice recommendations. Storage/compute provision can suit a range of workloads and has simple scaling. RDS allows data to be encrypted at rest and in transit for security.
- Amazon RDS can work with AWS Lambda to automate transit of encrypted backups to on premises server daily.
- Amazon Aurora is fully managed by Amazon RDS, which automates time-consuming administration tasks like hardware provisioning, database setup, patching, and backups.

Form Creation Architecture

•Simple web application that will connect to an API, allowing the creation of forms



•POST request will trigger the first set of step functions which will create a new table in the database, followed by another lambda which will take the stored HTML skeleton and add the required fields, then add it to an S3 bucket.



•once the data is inside the cloud it is then secured by AWS.

•Step functions are triggered which will create a CloudFront distribution along with SSL certificate, and assign a one-time, pre-signed URL.

•To track user-interaction CloudWatch will monitor traffic to the distribution.

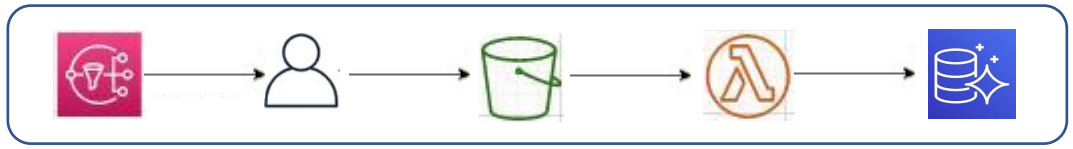
SNS, Hosting, Cloudwatch

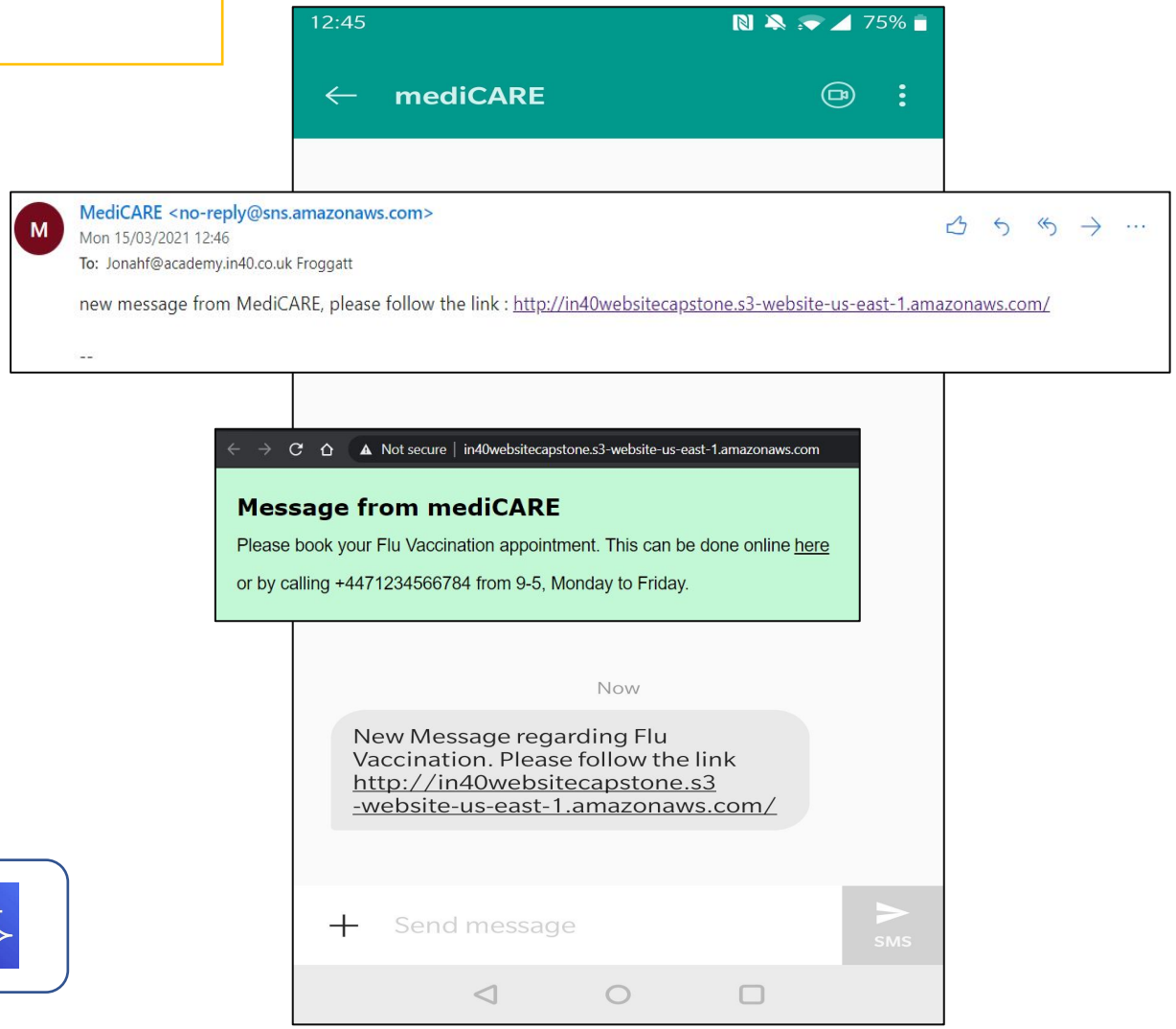
- Link to message sent via both email and SMS, as outlined in brief. This is done through SNS (Simple Notification Service), which sends a URL to each patient that requires a vaccination.

- Messages are hosted on a static website, with a separate URL for each patient. These websites are monitored using Cloudwatch, so MediCARE know who have viewed the message.

- Emails are very cheap to send, costing around £2 to send an email to each of the estimated 112,500 patients with an existing lung condition. SNS is used rather than SES (Simple Email service), as it is cheaper, and has all the functionality needed to send the link.

- The texts are a lot more expensive, costing over £3100 to send a text to each of the patients. This is the same for all of the AWS text services, and as its in the brief, this is the only option.



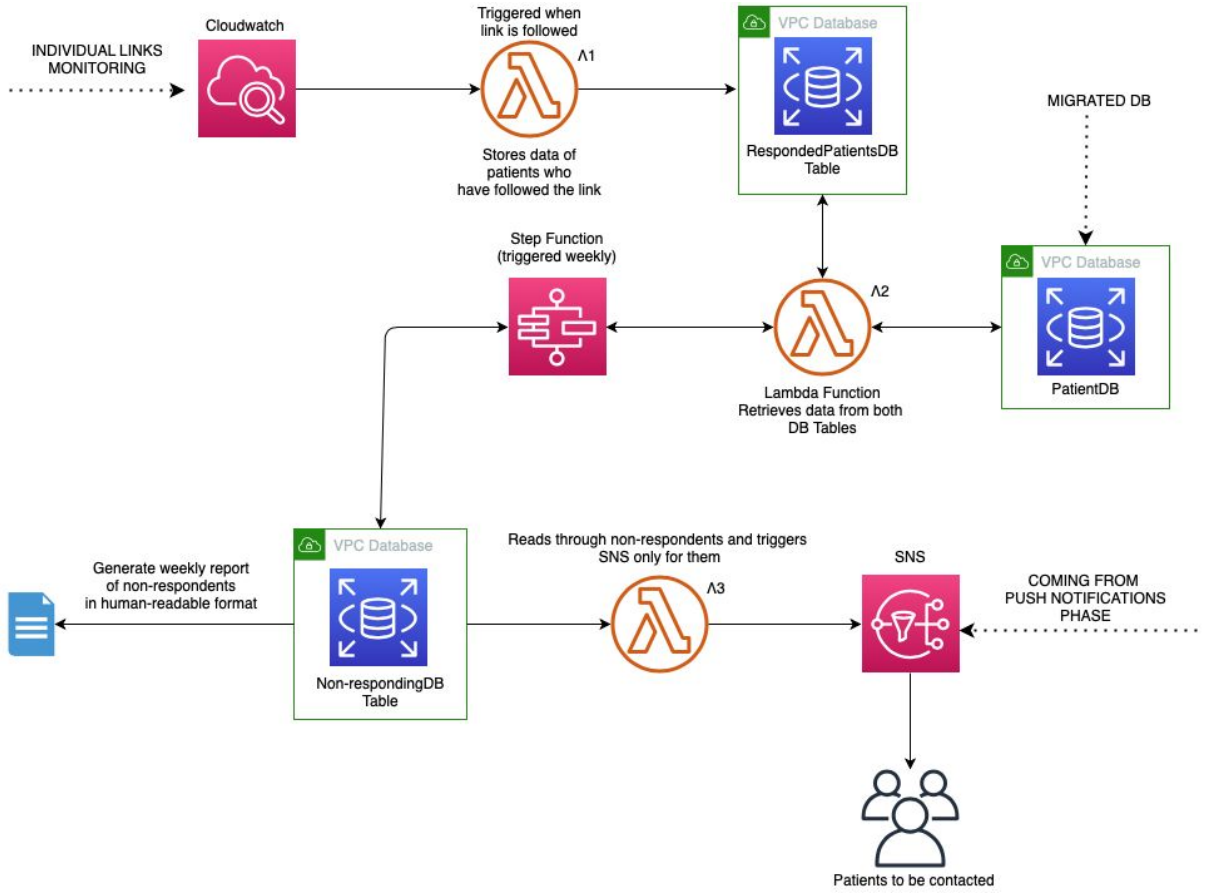


Report Building / Logging

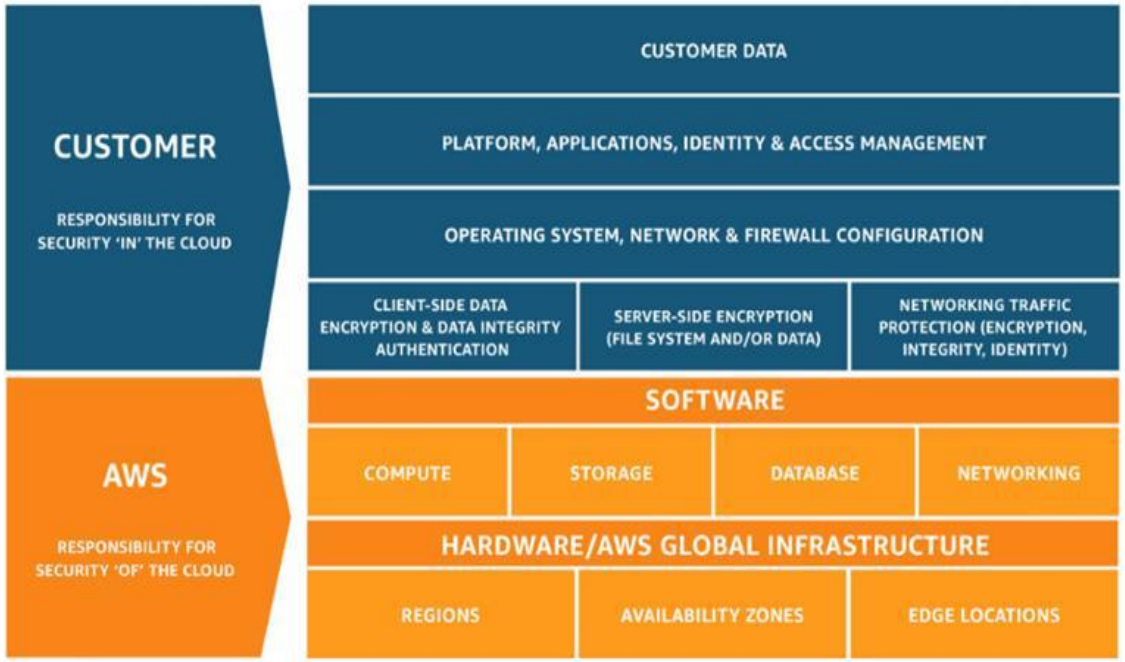
Purpose:
- Identifying all the patients that have not registered for the vaccination programme.

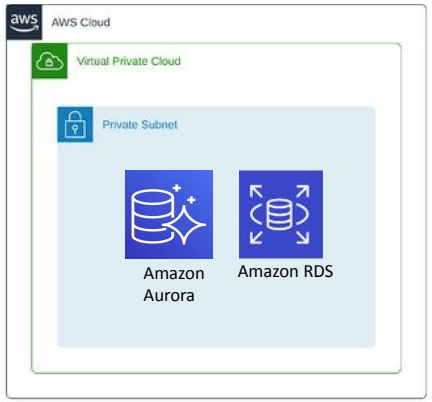
Aim:
- Building a separate database table with the non-respondent patients and repeat the push notifications process.
- Generating a weekly report that accounts for all the non-respondents left in the database.

Advantages:
- Utilise existing architecture.
- Avoid adding extra (and potentially redundant) services (such as SSRS & SES).
- Keep costs to a minimum.



Security, Data Encryption, IAM, MFA





Due to the nature of the company, security is vital and is a key part of the infrastructure. Security is implemented at all layers: -

- Focus is on securing the system: The responsibility of security and compliance is shared between AWS and the customer. So we need to focus on the security in the cloud, and Amazon will take care of the security of the cloud. Multiple VPCs are used to separate networking environments and ensure confidential data remains secure.
- Principle of least privilege is implemented. Two key services which help achieve this are AWS Identity and Access Management (IAM) and Multi Factor Authentication (MFA).
- Automate where possible: Step functions are triggered weekly, providing a report.
- Traceability is enabled: AWS CloudWatch and AWS CloudTrail are used for monitoring and logging.
- Costs are optimised: Amazon's Trusted Advisor 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

- We implemented our solution based on best practices outlined in the WAF and CAF
- We have adhered to the five pillars of the WAF and the six perspectives of the CAF
- Our architecture is tailored for the clients needs and covers all the brief, with a cost effective solution,
- We chose components and services such as; Aurora and serverless components.
- Because these services are managed by AWS, scalability, responsibility for maintenance logging and reporting, will be reduced for staff whilst allowing the ability to auto scale for demand.

[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]

[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].