REPORTING AND ALERTING MOBILE APPLICATION

(VERSION 1.0)

REQUIREMENTS SPECIFICATIONS

WEBRADR_Deliverables_D3A.8_03.docx

WEB-RADR INITIATIVE

WORK PACKAGE WP-3A

(HTTP://WEB-RADR.EU/WORK-PACKAGES/WP3A/)

TABLE OF CONTENTS

1. PURPOSE

The purpose of this User Requirements Specification document is to define and formally document the requirement specifications that the Reporting and Alerting Mobile Application system will satisfy, from a technical and system operations perspective related to the business processes it will support.

The Reporting and Alerting Mobile Application system will be created by Epidemico according to their development procedures.

2. SCOPE

This User Requirements Specifications applies to the pilot version of the Reporting and Alerting Mobile Applications (version 1.0) for MHRA (UK), Lareb (Netherlands) and Halmed (Croatia). The Reporting and Alerting Mobile Applications will be used by both Healthcare Professionals (HCPs) and patients and will be available in English, Dutch and Croatian.

This User Requirement Specification also includes requirements that would allow the development of a package of instructions and online tools to allow adoption by additional Member States of the Reporting and Alerting Mobile Application.

This specification will also cover the server hosted by Amazon Web Services and back-end database.

3. ROLES AND RESPONSIBILITIES

Role	Name/Company	Responsible for
Process/Data Owner (PDO)	- Epidemco - MHRA (UK) - Lareb (Netherlands) - Halmed (Croatia)	- certifies that the required & appropriate stakeholders have been involved in the creation of the document - certifies that the content of the document is accurate and complete
IT System Owner (IT SO)	Epidemico (application developer)	- certifies for his/her area of expertise that the content of the document is accurate and complete
Subject Matter Experts (SME's)	Please refer to WEB-RDAR Definition of Work document for list of team members and associated area of expertise.	- certifies for his/her area of expertise that the content of the document is accurate and complete
Validation Subject Matter Expert (VAL SME)	- MHRA (UK) - Lareb (Netherlands) - Halmed (Croatia) - Epidemico (application developer)	- responsible for organizing the execution of the validation activities
Data Privacy Officer	- MHRA (UK) - Lareb (Netherlands) - Halmed (Croatia) - EMA (EU)	- provides advice regarding data privacy risks, obligations, and mitigation strategies

4. DEFINITIONS

Brief technical and specific system definitions of acronyms and terms that may be used in this and other documents relating to this particular system are given below.

Term	Definition
ADR	Adverse Drug Reaction
Data management	The process of acquiring, storing, cataloging, retrieving, deleting and securing data.
HCP	Healthcare Professional
AWS	Amazon Web Services
HTTPS	Hypertext Transfer Protocol (Secure) - a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer.
XML	Extensible Markup Language - a markup language that defines a set of rules for encoding documents in a format which is both human-readable and machine-readable
API	Application Programming Interface
SOAP	Simple Object Access Protocol - a protocol specification for exchanging structured information in the implementation of web services in computer networks.

5. OVERVIEW OF THE SYSTEM

5.1 Intended Use of System

The Reporting and Alerting Mobile Application will be used by HCPs and patients to report Adverse Drug Reactions (ADRs) experienced whilst receiving medication or treatment for an illness. These reports will then be sent from the application to the appropriate local health authority via a back-end server managed by the app developers. The application will also be used by the health authorities to provide safety information directly to app users.

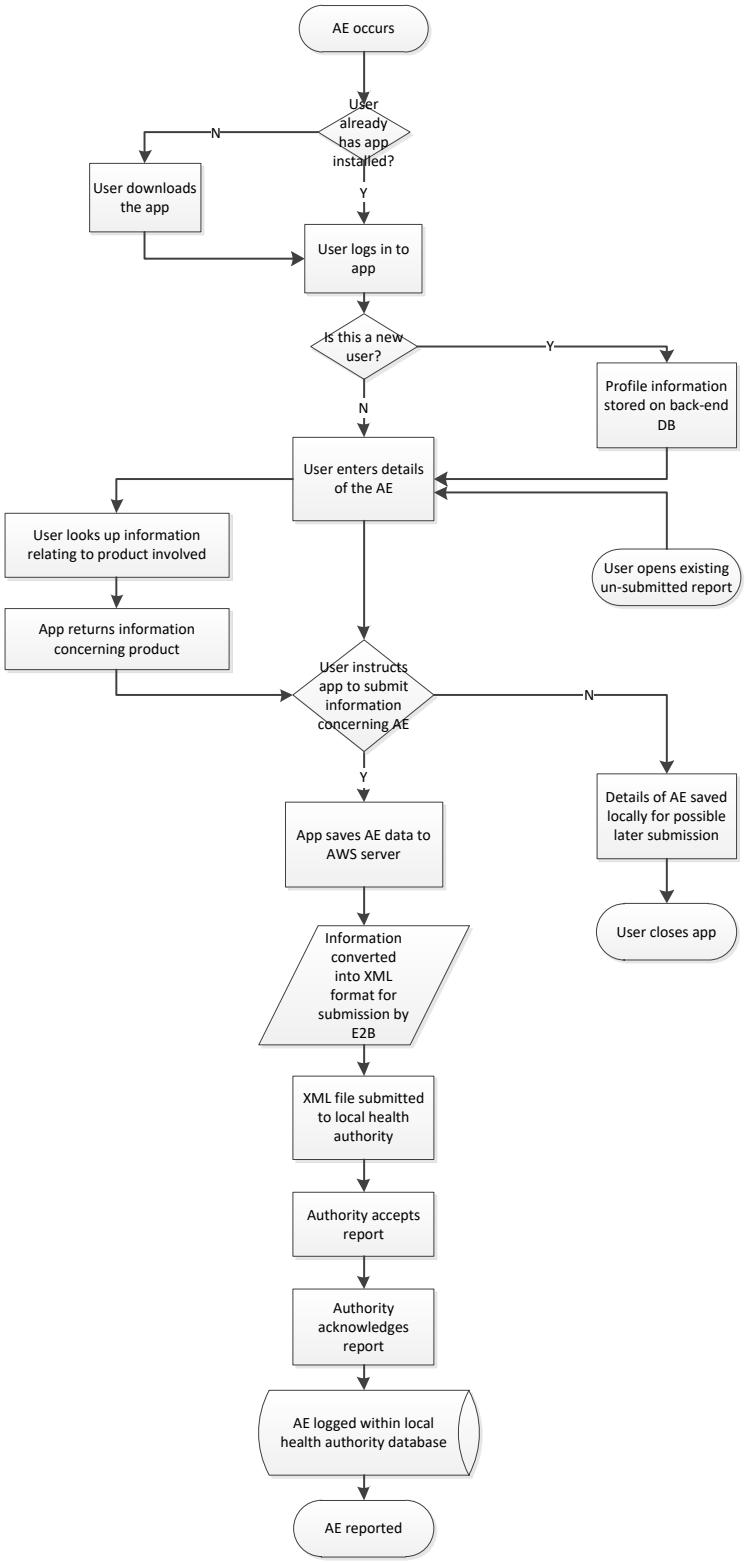
The Reporting and Alerting Mobile Application will be developed for use initially by local health authorities in three pilot member states. The app is intended to serve as an extension of existing ADR reporting tools and to augment existing reporting systems and processes.

The information flow for ADR reports submitted via the app will follow existing data flows for reports received from other drug safety data sources (e.g. spontaneous, observational).

The overall purpose of the data resulting from the app is to contribute to the understanding of a medical product's safety profile. The report form contained in the app has been designed to include only informational fields that support this purpose by enabling a comprehensive account of the event and patient, according to the health authority's requirements for ADR reporting and validation.

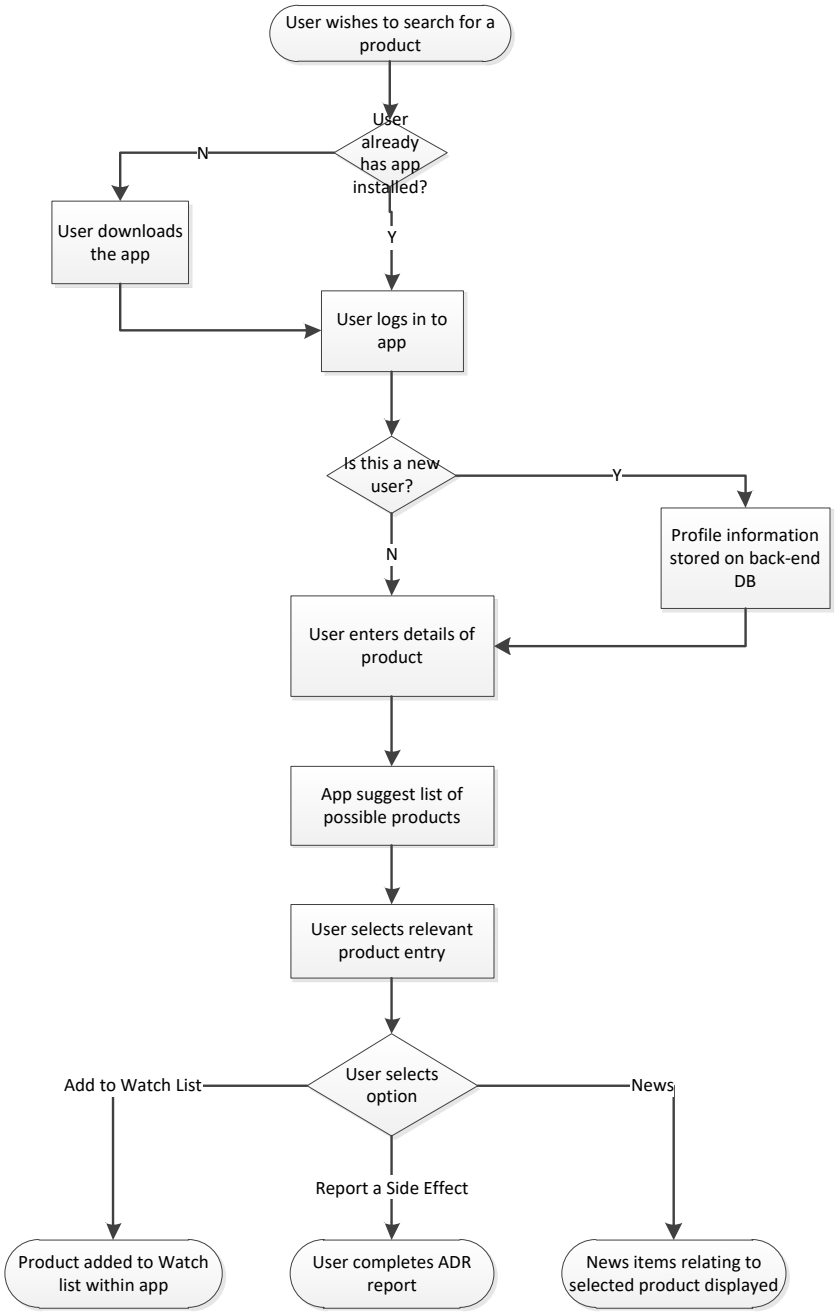
5.2 Description of the Business Processes

Adverse Drug Reactions (ADR) reporting

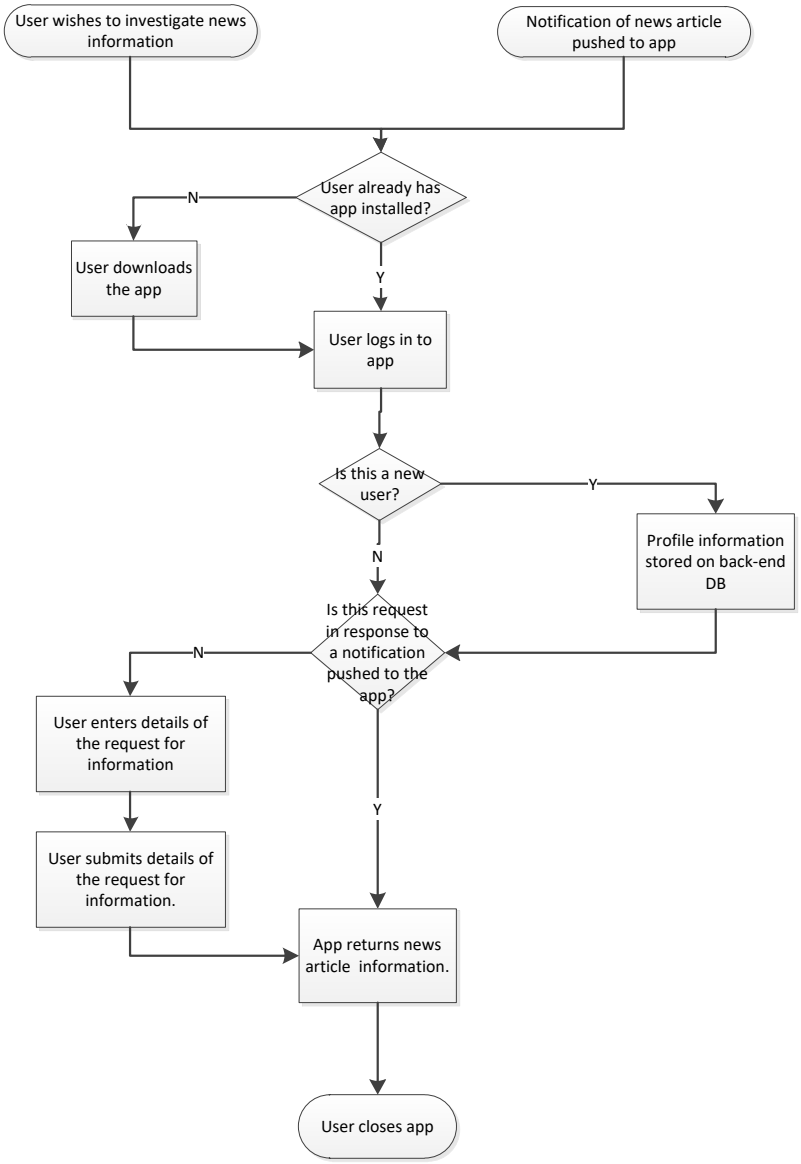


Only initial ADR reports will be submitted via the app - follow-up reports will be handled outside of the app

Product lookup



News article lookup

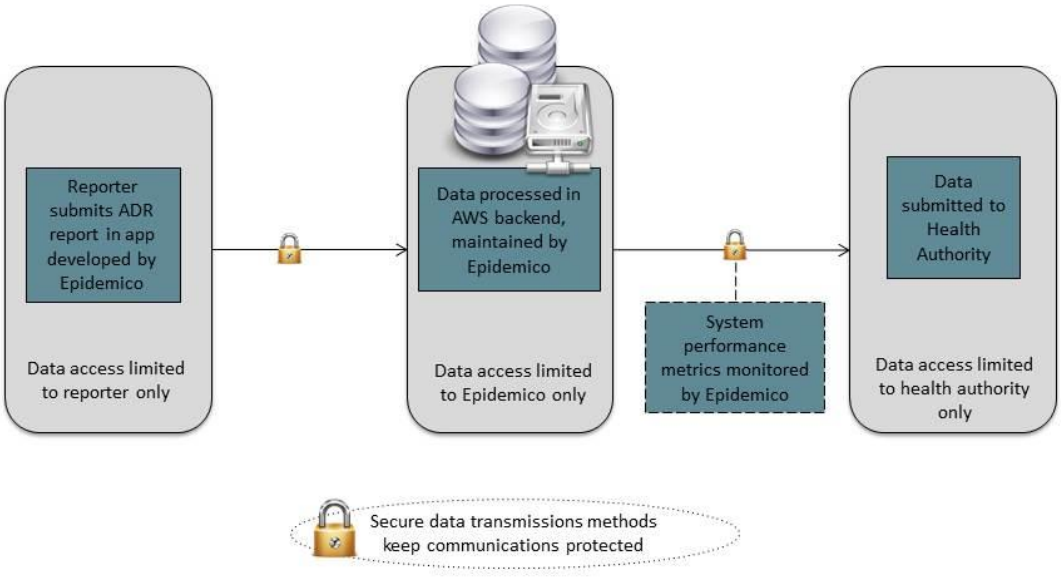


5.3 Description of the User Profiles

Users	Actions
Patients	• Download the app from App Store or Google Play • Launch app and inputs details of ADR • Launch app and configure a list of products to monitor (watch list) • Reviews information provided by the authorities (News) for the configured list of products • Submits the details to be sent to the Local Health Authority
HCPs	• Download the app from App Store or Google Play • Launch app and inputs details of ADR • Launch app and configure a list of products to monitor (watch list) • Reviews information provided by the authorities (News) for the configured list of products • Submits the details to be sent to the Local Health Authority
Local Health Authorities	• Updates configuration of the app as required to adhere to local data requirements • Receiving information regarding use of the app • Consumer of E2B reports submitted via API
Epidemico	• Performs maintenance and updates to app • Receives data on downloads of app • Collates information regarding use of app
AWS Server	• Automatically processes app data fields into report format (E2B xml) • Submits E2B reports to Local Health Authority API

5.4 Description of the Data

Dataflow Process



The mobile app will collect detailed ADR information as well as user and/or patient information relating to an ADR.

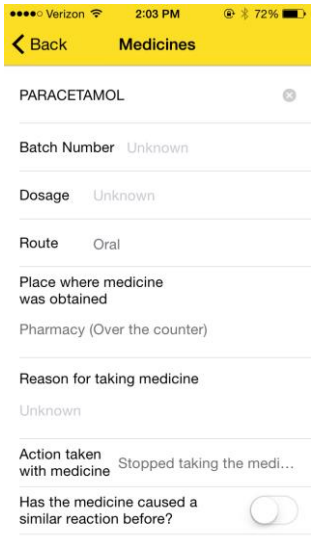
A user creates an ADR report in the app by filing in a series of fields to describe product and symptom information (see Figure 1).

This ADR report will be passed to a back-end server managed for Epidemco by AWS. This back-end server will then generate an XML file from the data within the report and submit this XML file via E2B to the relevant local health authority.

A record of each submitted ADR report is stored on the AWS server and a summary of the reports submitted by a user is available for that user to access at a later date via the app.

Uncompleted and un-submitted reports will be stored locally by the app for users to complete and submit at a later time.

Figure 1: Report form

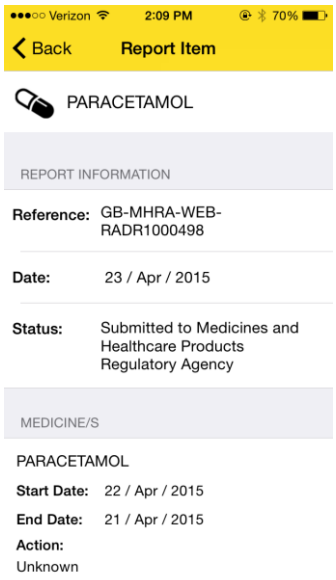


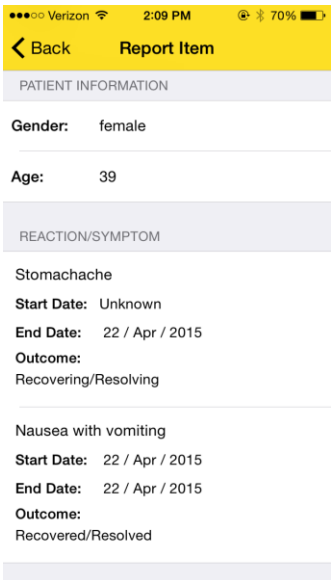
When the user completes and submits the report form, Epidemico securely stores the fields in a database, hosted on AWS's Ireland instance. Epidemico then processes these fields slightly to convert the data as needed for report submission to the health authority; for example, months are converted to years to submit the data in a format acceptable by the submission portal of the specific local health authority.

Next, Epidemico creates an XML file based on these formatted fields and sends it to the health authority's report submission portal via E2B, using web services provided by the Local Health Authority over HTTPS (secure hypertext transfer protocol). Once the XML file is received and successfully validated by the health authority, Epidemico does not have access to the formatted report nor to the health authority's report database.

Epidemico uses the original plain text fields provided by the app user to populate a summary of submitted reports in the user's own app (see Figure 2). These data are retrieved each time a user logs into the app and views his or her submitted reports.

Figure 2: Report Summary





Each local health authority will be considered the data controller for the reports they receive, while Epidemico will serve as the data controller of the raw text fields that are used to create the ADR reports.

It is anticipated that the health authorities will treat all personal identifiers contained in a report according to their own established protocol. Users can also choose whether their personal identifiers and contact information are included in the submitted XML reports to the health authorities (if the user provides this information) as only one mandatory field containing the patient's initials is required for report submission.

A thirty-minute time-out has also been implemented within the app to promote user privacy.

5.5 Interface with other Computer Systems

From System	To System	Bi-directional? (Y/N)	Data
Reporting and Alerting Mobile Application	AWS server	N	ADR information as defined in the Data Specification
AWS server	Local Health Authority	Y	XML file listing ADR as defined with ICH E2B standard, sent to Authority via HTTPS Message Delivery Notification messages and Acknowledgement message returned by Authority via HTTPS

6. USER REQUIREMENTS

6.1 Applicable Regulatory Requirements

The reports generated by the back-end server in response to a report being received from the app should meet the current E2B report guidelines (version R2).

Any data stored electronically must comply with the current data privacy regulations that apply in the country/region of the local health authority providing the app. The back-end server must also comply with these regulations, except where a suitable waiver is available and has been agreed.

6.1.1 Audit Trail Requirements

Users of the mobile app do not have the ability to change records already submitted and therefore there is no audit trail requirements for the application.

The standard Web server access logs as well as application-specific audit logs are kept for the back-end servers by AWS.

6.2 Operational Requirements

6.2.1 Business Process Requirements

There are no business process requirements covering the pilot app

6.2.2 Availability (Downtime and Maintenance) and accessibility

AWS do not provide any regular scheduled downtime for the back-end servers – AWS are generally able to perform updates and maintenance without downtime for the back-end servers.

Reference	Requirement
Availability	
R-OA-01	The app will not transmit data to the server in case of system failure for the back-end server.
R-OA-02	System “uptime available” for the AWS servers will be defined as 24 hours per day by 7 days a week.
R-OA-03	Monitoring will be implemented to alert the support team of any system outages or other system failures.
R-OA-04	Any scheduled system interruptions affecting the AWS servers will last no more than 1 hour
R-OA-05	AWS will provide a service health dashboard at http://status.aws.amazon.com/ to allow local health authorities to verify system operation
R-OA-06	For maintenance affecting the AWS back-end servers that require service interruptions, AWS will provide notification emails in advance.

6.3 Data Requirements

Data submitted from the Reporting and Alerting Mobile Application is processed on remote servers provided by AWS on behalf of Epidemico.

An XML file containing the ADR report is submitted using a REST API (such as SOAP) over HTTPS.

App data are encrypted in transit during submission to the local health authority. After submission, data are safeguarded according to the local health authority's security measures.

Epidemico has implemented several security measures to safeguard data and systems against destruction, alteration, loss, and intrusion. These safeguards are applicable to databases containing data collected by the Reporting and Alerting Mobile Application system. In addition, Epidemico has implemented network monitoring and logging procedures to oversee database activity and access.

The AWS server that receives data from the app is ISO 27001-certified.

Reference	Requirement
R-DA-01	Data from the local health authorities product lists should be available for the user to select any drug name (by substance or brand)
R-DA-02	Each local health authorities can define the mandatory fields it requires within the report. These will be made mandatory for the user to complete
R-DA-03	The current version of E2B guidelines must be followed
R-DA-04	Any additional fields or validation checks required by the relevant local health authority must also be included

Backup	
R-DB-01	System back up must not interfere/disrupt with data acquisition or data security activities
R-DB-02	Database snapshots of the back-end server will be captured nightly
R-DA-03	Application server images for the back-end server will be captured nightly
R-DA-04	All backup snapshots and images will be stored in a distributed data store by AWS
R-DA-05	Recovery of an image will be completed in less than one hour

IT Risks & Security	
R-DR-01	Users must provide login information each time they access the app
R-DR-02	A mandatory 30 minute logout is applied to the app when it is not being used. The user has to then log back in.

6.4 Interface and Connectors

Reference	Requirement
Interface with Other Systems	
R-IN-01	The AWS server must establish connectivity by submitting files via HTTPS to the relevant local authority services. The local authority will provide details of the necessary configuration settings on request.

6.5 Human Interface

Reference	Requirement
Human Interface	
R-HI-01	A home screen must be available for user navigation.
R-HI-02	A home screen includes a login page requiring email address and password.
R-HI-03	There will be an ADR reporting screen to log the details of the Adverse Drug Reaction(s) experienced.
R-HI-04	The system must be branded with the appropriate logo/colors for the local health authority.
R-HI-05	An acknowledgement/confirmation email must be provided for every report submitted. These will be sent direct to the user.
R-HI-06	The app will only allow the initial reporting of ADRs – follow-up information cannot be requested or submitted for reports already submitted.
R-HI-07	The app may contain distinct interfaces for logging a report, based on the profile that the reporter has created within the app
R-HI-08	The app will be available in multiple languages
R-HI-09	The app will not require multiple data logins as part of its operation
R-HI-10	The app will generate reminders of any un-submitted reports when users login
R-HI-11	The app will receive ‘push’ notification’ from the local health authority relating to items on the watch list of a user (if the local health authority systems are configured to provide such notifications)

6.6 Profiles and Roles (Access Control and Security Requirements)

Reference	Requirement
R-AC-01	The app is secure and able to recognize authorized users and grant them access to the system via user identity and password.
R-AC-02	The app will provide the ability for login information to be preserved across multiple sessions. This can be enabled or disabled either by the user or the relevant local health authority
R-AC-03	The back-end server shall generate activity logs and an audit trail accessible to the AWS team.
R-AC-04	The system security is able to handle a changing user population (e.g. new users, changing user types, user leaving).
R-AC-05	User lockout and failed access attempt entry will be recorded in the system audit trail and for the back-end server, a system administrator will be notified.
R-AC-06	Each user group will only be able to access their own data (reports, news articles and information requests)
R-AC-07	Passwords must follow the relevant security policies as defined by the local health authority providing the app.
R-AC-08	An email address can be assigned to only one single user profile within the app

6.7 Technological Requirements

Reference	Requirement
Specifications for the App	
R-TE-01	The application will be available for use on both Android and Apple iOS devices.

7. REFERENCES

References to specific issues of documents referred to or relied upon by this document are:

WEB-RADR WP-3A SharePoint document archive (password protected)

- https://sps-ext.nibsc.ac.uk/MHRA/imi/WP3a%20Mobile%20reporting%20platform/

WEB-RADR WP-3A technical documentation (password protected)

- https://sps-ext.nibsc.ac.uk/MHRA/imi/WP3a Mobile reporting platform/T3A.1 requirement gathering/Technical documentation

Amazon Web Services Cloud Compliance documentation

- http://aws.amazon.com/compliance/

EMA EudraVigilance Community Legislation and Guidance documentation (http://eudravigilance.ema.europa.eu/human/euPoliciesAndDocs03.asp)

- General Guidance Related to Electronic Reporting of ICSRs http://eudravigilance.ema.europa.eu/human/euPoliciesAndDocs03.asp#4

ICH Electronic Standards for the Transfer of Regulatory Information (ESTRI)

- Message Specification for E2B(R2) ICSR http://estri.ich.org/e2br22/ICH_ICSR_Specification_V2-3.pdf

8. APPENDICES

Appendix 1: Revision Log

DOCUMENT VERSION	DATE OF CHANGE	REASONS FOR THE CHANGE
1.0	09 October 2015	First version