AUA-AQUA Data Pull-Push Technical Overview
# Table of Contents

I. Introduction: .................................................................................................................................................. 2
   A. Data PULL - RPC Data Extraction Utility installed at participating practice/group: .................. 2
   B. Data PUSH – No RPC Data Extraction Utility installed at participating practice/group: .......... 2
   C. AQUA Dashboard Application hosted at US AWS Cloud: ................................................................. 3

II. FIGmd Solution Components: .................................................................................................................... 4

III. Data Flow Diagram- Data PULL: ............................................................................................................. 5

IV. Data Flow Diagram- Data PUSH: ........................................................................................................... 6
I. Introduction:

There are 2 Main ways of submitting data for the AQUA Registry, viz. Data PULL and Data PUSH:

A. Data PULL - RPC Data Extraction Utility installed at participating practice/group:
   - FIGmd sends Registry Practice Connector (RPC) installer to participating provider’s IT staff so that provider’s authorized IT personnel can install RPC in provider’s environment under his/her credentials.
   - RPC is installed as Service on server selected by the IT personnel of the practice/group.
   - The IT personnel also creates a read-only account to connect to its EHR database.
   - RPC is then configured to start a nightly job to extract all available clinical EHR data for all patients of all participating providers from the EHR,
   - The extracted data is first stored in a file on the practice/group server in encrypted, compressed format.
   - Another scheduled job then pushes it to the FIGmd registry database hosted on Amazon Web Services (AWS) cloud, which is outside of the practice/group’s IT system.
   - The Data is stored in AQUA Clinical Data Repository (CDR) Warehouse.
   - FIGmd mapping team then maps this data from CDR into the AQUA Datamart using the AQUA Registry Data Dictionary (DD). The mapping load on participant is far less than that involved in a Data PUSH method.
   - Participant only helps the FIGmd mapping team in the mapping exercise

B. Data PUSH – No RPC Data Extraction Utility installed at participating practice/group:
   - No RPC installation required at participant’s end.
   - Participant will send EHR data to AQUA AWS Data Warehouse via SFTP (SSL/TLS), Web Service or TCP Tunnel (VPN, etc.).
   - The data is sent in a pre-determined format (CDR Layout Template) to the Registry by the participant.
   - The Participant takes on mapping responsibilities for mapping their own EHR data to elements in the CDR Layout Template.
   - Data submitted by the participant is stored in AQUA Clinical Data Repository (CDR) Warehouse.
   - FIGmd mapping team then maps this data from CDR into the AQUA Datamart using the AQUA Registry Data Dictionary (DD). Some help is required from the participant to complete the final mapping.
C. AQUA Dashboard Application hosted at US AWS Cloud:

- FIGmd processes the data present in AQUA Database in AWS cloud environment.
- FIGmd allows participating providers to see dashboard that details performance of each participating provider.
- The AQUA Registry Dashboard gives snapshot of how a practice/group/provider is performing against the benchmark for each measure.
- FIGmd also supports PQRS submissions for the participating providers.
## II. FIGmd Solution Components:

<table>
<thead>
<tr>
<th>Category</th>
<th>RPC</th>
<th>Registry Dashboard Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who installs it</td>
<td>Participant practice/group Admin under his/her credentials</td>
<td>FIGmd</td>
</tr>
<tr>
<td>Hosted at</td>
<td>Practice/group environment</td>
<td>AQUA Registry hosted in AWS</td>
</tr>
<tr>
<td>Installed by</td>
<td>Practice/group IT admin</td>
<td>FIGmd</td>
</tr>
<tr>
<td>Accessed by</td>
<td>Only by practice/group IT admin &amp; FIGmd for Troubleshooting</td>
<td>Participants via Web browser; no direct access to data.</td>
</tr>
<tr>
<td>Incoming connections</td>
<td>RPC Management server for initial setup and data extract management.</td>
<td>Data load from RPC to AQUA CDR and then to AQUA data mart</td>
</tr>
<tr>
<td>What does it connect with?</td>
<td>EHR database with read-only account</td>
<td>Data processing within AWS cloud only</td>
</tr>
<tr>
<td>Does it access PHI?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Does it store PHI?</td>
<td>Yes, on practice/group server in compressed, encrypted format before upload.</td>
<td>Yes, a provider sees only his/her data based on role setup in dashboard portal</td>
</tr>
<tr>
<td>Outgoing Connections</td>
<td>AWS cloud to Clinical Data Repository (CDR) database of AQUA Registry</td>
<td>Browser access by participating providers</td>
</tr>
<tr>
<td>HW required</td>
<td>Processor: 1 GHz, 2 GB memory during scheduled data extraction and upload jobs. Hard Drive: 1 GB of free space, Broadband Internet Access.</td>
<td>Any web browser</td>
</tr>
</tbody>
</table>
III. Data Flow Diagram - Data PULL:

Data Pull Scenario

Registry in AWS

Mapping Analyst

RPC Management Server

Clinical Data Repository (CDR)

Registry Practice Connector (RPC)

EMR, Claims, and/or Billing Database(s)

Authorized Practice User

Enterprise Quality Management Server

Encryption for data in transit

256-bit Rijndael key

Port: XXXX

https://Port 443

2048-bit RSA key

Key Managed by Encryption Server Provider

- Data Marts
- Registry Quality Reporting
- Registry Dashboard

Microsoft Transparent Data Encryption (TDE)

128-bit Bit locker local / 256 EBS Network Drive encryption

Authorized Practice User

Data Pull Scenario

Registry in AWS

Mapping Analyst

RPC Management Server

Clinical Data Repository (CDR)

 Registry Practice Connector (RPC)

EMR, Claims, and/or Billing Database(s)

Authorized Practice User

Enterprise Quality Management Server

Encryption for data in transit

256-bit Rijndael key

Port: XXXX

https://Port 443

2048-bit RSA key

Key Managed by Encryption Server Provider

- Data Marts
- Registry Quality Reporting
- Registry Dashboard

Microsoft Transparent Data Encryption (TDE)

128-bit Bit locker local / 256 EBS Network Drive encryption

Authorized Practice User

Enterprise Quality Management Server

Encryption for data in transit

256-bit Rijndael key

Port: XXXX

https://Port 443

2048-bit RSA key

Key Managed by Encryption Server Provider

- Data Marts
- Registry Quality Reporting
- Registry Dashboard

Microsoft Transparent Data Encryption (TDE)

128-bit Bit locker local / 256 EBS Network Drive encryption

Authorized Practice User

Enterprise Quality Management Server

Encryption for data in transit

256-bit Rijndael key

Port: XXXX

https://Port 443

2048-bit RSA key

Key Managed by Encryption Server Provider

- Data Marts
- Registry Quality Reporting
- Registry Dashboard

Microsoft Transparent Data Encryption (TDE)

128-bit Bit locker local / 256 EBS Network Drive encryption
IV. Data Flow Diagram - Data PUSH:

- **Data Push Scenario**
- **Clinical Data Repository (CDR)**
- **Clinical Data Upload Server**
- **Registry in AWS**
- **EMR, Claims, and/or Billing Database(s)**
- **SFTP Server/Client**
- **Registry Quality Reporting**
- **Registry Dashboard**
- **Data Marts**
- **Registry in AWS**
- **Encryption for data in transit**
  - **https://Port XXXX 2048-bit RSA key**
- **Practice / Provider**
- **Supplied Data Feed**
- **Authorized User**
- **Enterprise Quality Management Server**
- **Key Managed by Encryption Server Provider**
- **128-bit Bit locker local / 256 EBS Network Drive encryption**
- **Microsoft Transparent Data Encryption (TDE)**
- **EMR, Claims, and/or Billing Database(s)**
- **SFTP Server/Client**
- **Copyright@2016**