ClaimsXten Cloud Editing Service (CCES)

**Security Diagram and Additional Details**

* Palo Alto firewall will have all security rules and policies activated according to CHC InfoSec guidelines
* All HTTPS traffic will need to be encrypted using TLS 1.2 protocol between all nodes (e.g. even last leg between ELB and CXT server needs to be encrypted)
* Only private IP address ranges will be allowed for communications between Aetna/DirectConnect and AWS hosted CXT application servers
* Data encryption in Oracle database decision - EBS level or TDE, still pending POC completion

**Web Service (request/reply) Data Flow for transactional claim process (REG)**

* Customer – Aetna, customer data center located in Windzor/CT and Middletown/CT
* **Web Service initiated from Aetna DC to AWS/AMS CHC owned VPC via Private Link service**



**SFTP file transfer from Aetna DC to AWS/AMS CHC owned VPC - use CHC Corporate GlobalScape SFTP server in Airpark**

* On-premise CXT pushes PGP encrypted and compressed files hourly to GlobalScape SFTP server over VPN/Internet
* Cloud CXT pulls files from the same SFTP server directly to the server mounted EBS file system (encrypted)
* Paid Loader process discovers files on local server and loads claims into ODS (RDS Oracle)
* GlobalScape internal connection:
* PROD - [mftinternal.emdeon.net](http://mftinternal.emdeon.net/) (10.140.47.17) (we should use this one from inside of our VPC for production)
* CERT - cert.mftinternal.emdeon.net (10.140.66.57 (we should use this one from inside of our VPC for POC and non-production)
* GlobalScape external (from internet) connection:
* PROD - [mftgateway.changehealthcare.com](http://mftgateway.changehealthcare.com/) - this one is for Aetna to use for production.
* CERT - cert.mftgateway.changehealthcare.com -  this one is for Aetna to use for POC and non-prod



**High Availability Deployment (Work In Progress)**

* Leveraging Multi-Az RDS deployment, Multi-Az application servers design and backup replication via S3 bucket to a DR AWS Region



**One-time historical claims data transfer and loading process**

Goal – transfer 3 years of production claims from Aetna production to the CHC Aws hosted CXT instance, load data into CXT ODS. Data is needed to establish CXT claim history for the accurate CXT rules firing.

****

1. Aetna DBA initiates CXT production data extract from Oracle ODS database inside Aetna data center. Data contains PHI claim information. Oracle DataPump technology and custom export configuration is used
2. Export data files are available for transfer, files are compressed and encrypted using PGP technology
3. Aetna DBA transfers files via private AWS DirectConnect link over Aetna owned S3 bucket. AWS CLI used to initiate transfer.
4. File transfer to S3 bucket is complete. S3 bucket is encrypted and permitted to access by the dedicated CHC user account (MFA is required).
5. CHC DBA initiates transfer from Aetna S3 bucket to EC2 node located in CHC VPC. CHC DBA uses AWS CLI to start the transfer
6. Once file transfer is complete all files become available on EC2 locally attached storage (encrypted EBS)
7. CHC DBA starts Oracle DataPump import process using custom import configuration. Content of data files loaded to Oracle RDS database.
8. Once all the steps are successfully completed and data integrity and data quality validated in Oracle RDS (e.g. verify application operational state via smoke test), all copies of data files are removed from Aetna data center location, AWS S3 bucket and CHC EC2 server
9. Done