Dear eClaimLink User,

As part of the ongoing enhancements on the eClaimLink technical platform we would like share with you the latest updates on the systems and policies taking effect in May 1, 2015.

I – Data archiving guidelines

In an effort to ensure high performance and responsiveness for the Dubai Health Post Office (DHPO) especially with the introduction of real time transactions (eReferral, eRx, PersonRegister), eClaimLink will be implementing a new archiving policy. Archived transactions will be transferred to a separate copy of the DHPO called Dubai Health Post Office Archive (DHPOA) based on the timelines listed below. DHPOA will be equipped with web services to enable the users from searching and downloading their archived transactions at any time.

Transaction	Period (days)
ClaimSubmission RemittanceAdvice ClaimResubmission	395
PriorRequest PriorAuthorization	395
eRxRequest eRxAuthorization	395
eReferral	395

- Archiving frequency = daily
- Time stamp = Transaction Date

DHPOA web service specifications will be published and circulated shortly.

II – eClaimLink DHPO new web services

New eClaimLink infrastructure was deployed to ensure higher performance and availability for the DHPO and eClaimLink applications. For the past month, a DHPO instance was implemented on the new infrastructure and tested to ensure the quality and performance of the new setup.

Migration to the new DHPO web services will be done through a 3 month transition period where eClaimLink directly integrated users will be able to utilize the existing web services as well as the new web services to manage their transactions to and from the post office. The transition period will end on [01/05/2015] and the old web services will be deactivated, and all users are expected to be functioning completely on the new web services.

Technical steps for the transition between the old and the new web services:

- Web services and web service methods on the new DHPO are identical to the existing web services being utilized. (no changes are required on this level)

New Web Services links:

- Web Services Address: https://dhpo.eclaimlink.ae/ValidateTransactions.asmx
- Web Services WSDL: https://dhpo.eclaimlink.ae/ValidateTransactions.asmx?wsdl

- An updated web service integration guide with the new links will be published on the portal
- Please be reminded to use HTTPs requests for all the DHPO web services and eClaimLink page links, as HTTP forwarding to HTTPS will not be supported after (01/05/2015)
- Documentation can be found through the path: **eClaimLink > DHD > Documentation >** Documentation: **DHPO WebService Specification 2015-02-04** (direct link) *Please log in for access.*

III – eClaimLink transactions decimal point restrictions

eClaimLink Schema fields with type (Float) will be updated to (Decimal) to eliminate cases where failure to upload a transaction is caused by the estimated value stored within a field from type (Float).

Technical explanation
DECIMAL and FLOAT are both used to store numerical values. But they have the following main differences:

- DECIMAL(p,s) stores values with the decimal point fixed at the position of s (scale) digits from the right. The total number of decimal digits is also fixed as p (precision).
- FLOAT(n) stores values with the decimal point floating based on the value. The number of bits used to store the mantissa part is fixed as n.
- If the input value of DECIMAL(p,s) has more digits after the decimal point than the scale s, the value will be rounded to the scale s.
- If the input value of FLOAT(n) has more total digits (mantissa) than what n bits can store, the value will be rounded to fit the storage size.
- If the input value of DECIMAL(p,s) has more digits before the decimal point than p-s, SQL Server will give you an over-flow error.
- If the input value of FLOAT(n) is too big that the exponential part goes over the positive limit, SQL Server will give you an over-flow error.
- If the input value of FLOAT(n) is too small that the exponential part goes over the negative limit, SQL Server will give you an under-flow error.

No effects are expected on user systems therefore with no need for IT changes. The change will only affect the data storage format on the DHPO.

IV – eClaimLink Observation Field Standardization

In order to standardize the structure and content of the Observation fields within the transactions, EDSC has published a detailed document outlining details of populating the fields related to all the possible observation types.

- Documentation can be found through the path: **eClaimLink** > **DHD** > **Documentation** > **EDSC Releases**: **eClaimLink EDSC Release V5 2014-04-20** (direct link)

All Observation fields will be mandatory as per the document, where default values must be utilized when needed as per the published guidelines. New validation rules in the DHPO will assure that these guidelines are followed. Non-Compliant transactions will be rejected.

V – eClaimLink Remittance Advice response

Payers are expected to have 100% remittance advice responses to all of the claim submissions they receive. New denial codes have been added to cover the cases where Claims are recalled by a provider due to wrong submission.

Code	Description
CLAI-018	Claims Recalled By Provider Denial code used to notify the Clinician or Pharmacist that the ClaimSubmission has been recalled by the submitting provider.
WRNG-001	Wrong submission, receiver is not responsible for the payer within this transaction submission. Denial code used to notify the Provider that the payer within the transaction is not under the receiver's responsibility.

VI – Password policy

Part of the security enhancements on the eClaimLink platform will require a strong password with proper use from the eClaimLink community. The password policy will be mandatory for both the eClaimLink portal as well as the web services utilized to communicate with the DHPO.

Password structure

- Password length must be at least eight characters.
- Password must contain at least one numerical digit.
- Password must contain at least one special character, e.g. ! @ #

Password duration

- For better security measures, password is expected to be changed every 90 days.

Password best practice

- Never share a computer account
- Never use the same password for more than one account
- Never tell a password to anyone, including people who claim to be from customer service or security
- Never write down a password
- Never communicate a password by telephone, e-mail or instant messaging
- Being careful to log off before leaving a computer unattended
- Changing passwords whenever there is suspicion they may have been compromised
- Operating system password and application passwords are different

Best Regards,

Information Desk Officer

eClaimLink
https://www.eclaimlink.ae/
6005 22004