Centers for Medicare & Medicaid Services (CMS)
7500 Security Blvd
Baltimore, MD 21244-1850

HIPAA Eligibility Transaction System (HETS)
Health Care Eligibility Benefit Inquiry and Response (270/271)
R2016Q300
Web Services
Checklist for Successful Connections

FINAL

Version: **1-0**

Last Updated: May 2016

TABLE OF CONTENTS

1 SOAP 1

1.1 Protocol Level 1
1.2 Application Level 1
1.3 Body Elements of Request 1
1.4 Other 1

2 MIME 2

2.1 Protocol Level 2
2.2 Body Elements of Request 2

APPENDIX A - REVISION HISTORY 3

LIST OF TABLES

Table 1 - Document Revision History 3

All HETS 270/271 Web Services Submitters must ensure they are utilizing an originating IP address and certificate that is on file with CMS and listed on your current HETS 270/271 Trading Partner Agreement (TPA). If necessary, submit an amended TPA and allow adequate time (4-6 weeks) for CMS to update your organization's technical profile.

1 SOAP

1.1 Protocol Level

- Ensure that your organization is using TLS v1.2. HETS will aggressively enforce this requirement effective in the R2016Q300 release.
- Ensure that your organization is using an approved Cipher Suite. The list of approved Cipher Suites is documented in the HETS SOAP/MIME Connectivity Guide. HETS will aggressively enforce this requirement effective in the R2016Q300 release.
- Make sure the certificate is issued by one of CMS' approved intermediate CAs and is not expired or revoked.

1.2 Application Level

- The wsu:Timestamp and Payload elements must be signed and SHA-256 must be used as the Digest Method and Signature Method algorithms. HETS will aggressively enforce this requirement effective in the R2016Q300 release.

1.3 Body Elements of Request

- Ensure the PayloadID is Version 1 UUID. HETS Redesign requires the element adhere to the CAQH CORE guidelines documented in Rule 270. HETS will aggressively enforce this requirement effective in the R2016Q300 release.

1.4 Other

- When HETS is signing the outbound response, it will use a SHA-256 algorithm.

2 MIME

2.1 Protocol Level

- Ensure that your organization is using TLS v1.2. HETS will aggressively enforce this requirement effective in the R2016Q300 release.
- Ensure that your organization is using an approved Cipher Suite. The list of approved Cipher Suites is documented in the HETS SOAP/MIME Connectivity Guide. HETS will aggressively enforce this requirement effective in the R2016Q300 release.
- Make sure the certificate is issued by one of CMS' approved intermediate CAs and is not expired or revoked.

2.2 Body Elements of Request

- Ensure the PayloadID is Version 1 UUID. HETS Redesign requires the element adhere to the CAQH CORE guidelines documented in Rule 270. HETS will aggressively enforce this requirement effective in the R2016Q300 release.

APPENDIX A - REVISION HISTORY

Table 1 provides a summary of changes made to this document.

Table 1 - Document Revision History

Version	Date	Description of Changes
1-0	05/25/2016	Initial Version