Beacon Rebate Model FAQs: Top Priority for CHCs

Table of Contents

General

1. **How is the Beacon platform different from the 340B ESP platform and does my covered entity still need to use 340B ESP?**

The 340B ESP platform supports manufacturers' contract pharmacy policies and will continue to do so by enabling covered entities to make contract pharmacy designations, apply for wholly owned contract pharmacy exemptions, and submit 340B claims data. Contract pharmacy eligibility from 340B ESP will be effectuated through 340B claims validation in Beacon, and utilization for ineligible contract pharmacies will remain ineligible for 340B rebate payments.

In addition to retail claims data, Beacon also supports the collection of claims for utilization across separately payable product administrations, and outpatient product administrations for subsequent 340B rebate payments. Although covered entities will not be required to submit 340B claims data to 340B ESP for products that are part of the 340B Rebate Model, please note that pharmaceutical manufacturer policies may require the continued submission of claims data in 340B ESP for products not in scope for the 340B Rebate Model.

2. **Are the Beacon 340B Rebate Model and Beacon MFP (Maximum Fair Price) platforms integrated?**

No, the two user interfaces are not integrated. Users will log in to Beacon 340B Rebate Model separately from Beacon MFP. However, the 340B rebate data created in the Beacon

340B Rebate Model is integrated with Beacon MFP in order to account for the de-duplication of MFP and 340B rebates.

3. **Will my covered entity continue to have access to 340B pricing through my wholesaler for products in the 340B Rebate Model?**

Covered entities will no longer have access to 340B pricing through their wholesalers for those products in the 340B Rebate Model. Please visit the Resources page to view manufacturer policies. For products included in the 340B Rebate Model, covered entities will purchase these products at a commercial price (e.g. wholesale acquisition cost or WAC) and then receive a rebate payment on the purchase once 340B claims have been submitted, validated, and accumulated in Beacon.

4. **Does my covered entity have to register for a Beacon account if my covered entity is already utilizing a virtual inventory model?**

For all drugs included in the 340B rebate pilot, the only way covered entities will be able to access 340B discounts will be through manufacturer rebates processed through their vendor Beacon 340B. Covered entities' 340B wholesaler accounts will be loaded with the WAC price for the 340B rebate pilot drugs. Access to 340B rebate payments is created by submitting valid 340B eligible dispense or administration data to Beacon. Please review the manufacturer policy or the NDC list of products in scope for the Beacon Rebate Model in the Beacon Resources page.

5. **How does Beacon associate 340B claims with 340B purchases shipped to a contract pharmacy location?**

Claim submissions dispensed through a 340B contract pharmacy location will only be associated with purchases made by the covered entity and shipped to the same 340B contract pharmacy location.

Beacon Account Creation

1. **Does Beacon require that my covered entity register with the same authorized user from ESP or Beacon MFP?**

The same individual who registered a covered entity account on 340B ESP or a dispensing entity account on Beacon MFP is not required to register the account with Beacon. The individual registering a covered entity account on the Beacon Rebate Model must be authorized to do so, verify their email, and have all required information and documentation to complete account registration.

Updated as of 12/5/2025

2. **What information is required to register an account with Beacon 340B?**

Covered entities can register an account with Beacon free of charge. A registering user must first establish affiliation with the 340B covered entity by providing an EIN, an IRS letter (e.g., CP575) with the entity address, Articles of Incorporation, and a W-9 (using the March 2024 revision) for the covered entity. This information is validated by a third party adhering to Know Your Business standards. Once validated, the registering user establishes their Beacon account credentials and sets up their multi-factor authentication (MFA). Following the successful enrollment of a 340B covered entity, the registering user or another user established as an Administrator must request and submit a Bank Letter from their US financial institution, including bank account information, for ACH payments. This occurs once logged into Beacon. The ACH information must be successfully verified as associated with the 340B covered entity prior to any 340B rebate payments.

3. **Can my covered entity complete Beacon 340B registration without bank account information?**

After completing the initial enrollment and registration, users establish their Beacon account credentials and their multi-factor authentication (MFA). Once logged into their Beacon account, the Beacon platform prompts the Administrator to provide and verify the banking details for their covered entity. This includes submitting a certified Bank Letter from its U.S. financial institution and providing the appropriate bank account information for ACH payments. This documentation must be successfully verified as associated with the 340B covered entity before 340B rebates can be paid.

4. **Does my covered entity have to complete Beacon 340B registration for each child site?**

Grantee covered entities must register each unique 340B ID; however, users may register and manage multiple covered entities within a single account. For health centers, this means registering each associated grantee site.

Data Submissions

1. **Does my covered entity have to submit data to Beacon 340B if my covered entity is already submitting data to ESP?**

Covered entities should review each specific manufacturer's policy to determine which products are in scope for 340B rebate payments. 340B claim submissions for products participating in the 340B Rebate Model can only be made in Beacon. Users who attempt to

submit 340B claims for 340B Rebate Model products in 340B ESP will be notified of the requirement to submit the 340B claims in Beacon, and the 340B claims will not be ingested into 340B ESP. However, products not in scope for 340B rebate payments may still require the submission of 340B claims data in 340B ESP.

2. **How does a pharmaceutical manufacturer use the 340B claims data submitted to Beacon 340B?**

340B claims data submitted by a covered entity, or TPA, are used to validate the eligibility of the dispense or administration for a 340B rebate payment. Validated 340B rebate data are also used to determine the MFP refund amount after accounting for prohibited duplication with 340B pricing. Furthermore, 340B claims data may be used to identify ineligible rebates on Medicaid and commercial utilization. Please review the policies posted in the Beacon Resources page for more information on the eligibility business rules used in the claims validation process.

3. **How frequently can my covered entity upload claims data to Beacon 340B?**

Beginning January 1, 2026, covered entities can submit 340B claims data to Beacon as soon as claims are qualified as 340B eligible by the covered entity or its TPA. 340B rebate payments can only be made following the submission and validation of 340B claims data to Beacon and covered entities are encouraged to submit the claims data in a timely manner. To avoid significant volumes of reversals and the associated complexity in reconciliations, covered entities should only submit final claims.

4. **How are inconsistencies in the unit of measure between pharmacy and medical claims resolved in Beacon 340B?**

Certain products may be billed using different units of measure when dispensed to a patient and reimbursed under the pharmacy benefit versus when administered to a patient and reimbursed under the medical benefit. For example, a product may be dispensed in milliliters but administered in milligrams. Beacon is configured to accept pharmacy and medical claims in pre-established unit volumes, and unit validations are performed prior to submitting claims data to ensure Beacon ingests the expected unit value for pharmacy and medical claims. Look up tables with unit validations are available online on the Beacon Resources page, and covered entities are encouraged to review these unit validations prior to submitting 340B claims.

5. **How are claim reversals submitted and processed in Beacon 340B?**

Submission of a claim to Beacon is a request for payment of a 340B rebate, and covered entities should only submit final claims. In the event that a previously submitted and

validated claim must be reversed, covered entities should submit the same claim detail with a negative unit amount. The negative unit amount will be used to reverse the positive unit amount of the earlier claim. Reversed 340B claims will offset payment of a similar number of units on future 340B rebate requests.

Claims Data

1. **How should my covered entity submit multiple administrations of the same product to the same patient on the same day?**

When multiple administrations of the same product are administered to the same patient on the same day, covered entities should ensure that each administration submitted is identified with a unique claim number. Wastage claims may be submitted as a separate claim and should be denoted using the HCPCS modifier code 'JW'. By including the 'JW' modifier, the claim will not be rejected as a duplicate claim submission.

340B Rebates

1. **Are 340B rebates paid on individual dispenses of a product or for purchases of the product? Can my covered entity reconcile 340B rebate payments back to claims submissions?**

Following the submission of eligible 340B claims data, 340B rebates will be paid in accordance with the payment information provided by the 340B covered entity. It is HRSA's expectation that a purchase is made at the WAC price through the 340B account prior to submitting the claims data to Beacon for a rebate payment. Users will have insight into the status of these rebates while their request is being processed. For example, a package of a product may contain 100 units, and a typical dispense of that product may contain 30 units. A 340B claim submission for 30 units will result in a 340B rebate payment that represents 3/10 of the package level 340B rebate amount.

Covered entities will be able to reconcile 340B rebate payments back to the submitted 340B eligible claims data. This information is available in Beacon to review as well as accessible through a downloadable data report.

2. **How does Beacon determine duplication across Medicare and Medicaid?**

Beacon utilizes data elements within the submitted claims data to identify potential duplication with MFP and Medicaid rebate requests. MFP rebate requests that are

duplicative with 340B rebate payments will be reduced to reflect the 340B price already made available to the dispensing entity. In instances where the MFP rebate has already been paid, a corresponding credit will be recorded with the MTF's credit/debit ledger. Duplication in Medicaid will be addressed by rejecting or reversing Medicaid rebates. Depending on state law, this rejection or reversal of the Medicaid rebate may result in changes to reimbursement for the covered entity.

Support

1. **Are there available resources for educating my covered entity?**

The Beacon Support Center hosts an array of content, including educational videos that range in topics from Account Registration to Data Submissions, step-by-step guides on utilizing Beacon, downloadable data templates to streamline the data intake process, and articles that help further elucidate Beacon functionality. Visit the Beacon Support Center and the Resources page to learn more.

2. **How should my covered entity educate our TPA/EMRs?**

Covered entities should encourage their TPA and EMR providers to review the Beacon Support Center. Support designed specifically for TPAs including articles and training sessions is available in the Beacon Support Center.

Security

1. **How does Beacon handle protected health information (PHI)?**

Data elements protected under HIPAA are de-identified through a HIPAA compliant hashing process known as SHA-3 hashing. An additional layer of security called a "salt" is applied prior to the hashing process and before any data is uploaded to Beacon. This process was granted an Expert Determination and meets the definition of a De-Identified Data Set under HIPAA. This means that Beacon does not collect or maintain identifiable PHI.

2. **How does Beacon ensure the security of submitted data and manage access control?**

Beacon supports physical, technical, and operational security protocols that are consistent with industry-standard security best practices. This includes secure transfer of data from clients to Beacon (e.g., data-in-transit encryption), secure storage of that data

once in Beacon (e.g., data-at-rest encryption), and secure network segmentation designed to ensure that data is protected in the inner most security ring of the Beacon environment. All of that is coupled with a least privilege access control model designed to limit access to data based on need alone. Visit The Beacon Trust Center to learn more about the security protocols in place today.

Before registering, administrators are associated with a Beacon account, and administrators must demonstrate authenticity by providing supporting documentation. This documentation undergoes a third-party review adhering to Know Your Business standards. Once approved, registered users establish a password and a Multi-Factor Authentication that meets Beacon's stringent criteria.

3. **How does Beacon manage data deletion and retention?**

All data associated with Beacon will be retained indefinitely. Any data purge or deletion requests from covered entities will be discussed and only approved after written authorization from all impacted parties. Visit The Beacon Trust Center to learn more about Beacon's data deletion and retention policies.

HIPAA and Privacy

1. **What data is de-identified for claims submissions, and how does Beacon regulate data integrity before submission?**

Rx number, product serialization number, and claim number are deidentified. This process was granted an Expert Determination and meets the definition of a De-Identified Data Set under HIPAA.

Data elements protected under HIPAA are de-identified through a HIPAA compliant hashing process known as SHA-3 hashing. An additional layer of security called a "salt" is applied prior to the hashing process and before any data is uploaded to Beacon. This occurs in local memory accessed by the user's browser, ensuring that no native PHI is submitted to Beacon.