



CAQH Endpoint Directory Work Group

Session #2

November 13, 2020
3:00 – 5:00pm ET

Antitrust Guidelines

- Participation at this meeting and any subsequent meetings is voluntary.
- The sponsors are responsible for preparing a written agenda for the meeting and preparing written minutes for the meeting.
- The Chairperson of the meeting or the moderator of each discussion group will ensure that discussion follows the agenda.
- Participants will not discuss matters of a competitive nature, such as nonpublic information regarding pricing, products, or customers.
- Any participant who believes the meeting is covering an area of a competitive nature should raise the issue with the Chairperson or moderator, with counsel for any of the meeting's sponsors, or with the participant's own counsel.

The meeting will be recorded to ensure accurate documentation



Session Outline

Time (ET)	Topic	Details
3:00-3:10pm	Welcome	<ul style="list-style-type: none">▪ Antitrust guidelines, roll call▪ Review session objectives and agenda topics
3:10-3:35pm	Straw Poll Results	<ul style="list-style-type: none">▪ Straw poll overview▪ Summary of areas of consensus vs. areas that require further discussion▪ Results by topic
3:35-4:10pm	Discussion: Topic #1	<ul style="list-style-type: none">▪ Privacy, Security and Data Policies, Provisions & Attestations
4:10-4:40pm	Discussion: Topic #4	<ul style="list-style-type: none">▪ Endpoint Hierarchy & Org IDs
4:40-4:50pm	Looking Ahead	<ul style="list-style-type: none">▪ Upcoming topics and session dates▪ Beta Testing opportunity
4:50-5:00pm	Next Steps	<ul style="list-style-type: none">▪ CAQH staff send draft attestation questionnaire to work group participants; participants review draft attestation questionnaire.▪ Participants discuss beta testing opportunity with their organization.▪ Attend next session: Tuesday, 12/1/20, 12:30-2:30pm ET.

Time (ET)	Topic
3:00-3:10pm	Welcome
3:10-3:35pm	Straw Poll Results
3:35-4:10pm	Discussion: Topic #1 – Privacy, Security and Data Policies, Provisions & Attestations
4:10-4:40pm	Discussion: Topic #4 – Endpoint Hierarchy & Org IDs
4:40-4:50pm	Looking Ahead
4:50-5:00pm	Next Steps

Work Group members were asked to complete a four-part straw poll survey

The Work Group provided feedback on topics that may require consensus discussion in order to finalize requirements for the CAQH Endpoint Directory. **Areas with lower levels of agreement are prioritized for further discussion during today’s session and subsequent sessions.**

Topic 1:
Privacy, Security, and
Data Policies, Provisions,
and Attestations

1. For each item listed below (related to privacy, security, data use, standards conformance, etc.), please indicate (a) if it is important for an organization to upload a document or provide a URL in support of that item, (b) if it would be helpful to include questions about the item on a standard attestation questionnaire, and (c) if there are particular elements within that item that your organization needs to see/verify.

	A It is important for organizations to upload a document or provide a URL in support of this item.	B It would be helpful to have organizations answer questions about this item on a standard attestation questionnaire.	C If there are specific elements within this item that your organization looks for, list below.
1. Privacy policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
2. Privacy policy by plan	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
3. State privacy notices	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
4. Individual privacy rights and forms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
5. Privacy policies related to BAAs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
6. Data policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
7. Terms of service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
8. Signatory to CARIN Code of Conduct	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
9. HIPAA privacy and security compliance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
10. HITRUST certification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>

Topic 2:
Conformance Testing

Topic #2: Conformance Testing

4. At a high-level, which of the following tests would you like to see completed by a third-party app vendor:

☐ Connectivity and security test (test connection using dummy client ID/secret key, etc.)

☐ Patient Access API test (successful and conformant query and display of response)

☐ Provider Directory API test (successful and conformant query and display of response)

☐ Display of response data in vendor application (UI screenshot upload matches with API response)

☐ Other

5. At a high-level, which of the following tests would you like to see completed by other payers:

☐ Basic endpoint status test (test that a payer's API is available)

☐ Connectivity and security (test connection using dummy client ID/secret key, etc.)

☐ Patient Access API test (successful and conformant query and response)

☐ Provider Directory API test (successful and conformant query and response)

☐ Other

6. Insert any comments you would like to share related to this topic. If related to a specific question above, please reference the question # in your comments.

Topic 3:
Revalidation Cadence

7. At what cadence would you like to see third-party app vendors be prompted to revalidate that the information they provided related to privacy, security, and data use is still accurate and current?

☒ Whenever a relevant policy or provision is updated.

☐ Based on a regular calendar/specified timeframe cadence.

☐ Hybrid: aligned to relevant policy/provision updates, but if no updates occur within a specified timeframe, prompt organization for revalidation.

☐ Upon connection request with a payer.

☐ Other

8. At what cadence would you like to see payers be prompted to revalidate that the information they provided related to privacy, security, and data use is still accurate and current?

☒ Whenever a relevant policy or provision is updated.

☐ Based on a regular calendar/specified timeframe cadence.

☐ Hybrid: aligned to relevant policy/provision updates, but if no updates occur within a specified timeframe, prompt organization for revalidation.

☐ Upon connection request with another payer.

☐ Other

9. At what cadence would you like to see third-party app vendors revalidate their app's conformance testing?

☐ After every app version update, including minor versions.

☒ After major app version updates only.

☐ Based on a regular calendar/specified timeframe cadence.

☐ Hybrid: aligned to app version updates, but if no updates occur within a specified timeframe, prompt organization for revalidation.

Topic 4:
Health Plan Identifiers
and Endpoint
Organizational Hierarchy

11. By which characteristic are your endpoints organized? Select all that apply.

☐ Payer/Carrier

☒ Line of Business

☐ Geographic Region

☐ Market

☒ Group/Plan/Product

☒ Use Case

☐ Functional Department (e.g. claims system, provider network, etc.)

☐ Other

12. Understanding organizational hierarchy is important for determining how to represent organizations in the directory, and how to resolve organizational information to an associated endpoint. Please order the following concepts from highest to lowest, with the top concept being the highest level of how your systems organize information.

☒ 1. Payer/Carrier

☒ 2. Line of Business

☒ 3. Geographic Region

☒ 4. Market

☒ 5. Group/Plan/Product

☒ 6. Use Case

☒ 7. Functional Department (e.g. claims system, provider network, etc.)

☐ 8. Other

Topic 5:
Overall Rating

Additional Feedback

17. How important is it to your organization to be able to see an overall rating that indicates how organizations scored in areas related to privacy, security, and data use, and conformance testing?

☐ Very unimportant

☐ Unimportant

☒ Neutral

☐ Important

☐ Very Important

18. List any additional consensus topics you feel the work group should discuss. Please provide context.

19. I will share the following items with CAQH staff for their reference (send to endpointdirectorywg@caqh.org):

☒ General privacy policy

☐ Terms and conditions



☐ Privacy policies related to BAAs

☐ Data policy

☐ Architecture diagram of your endpoints

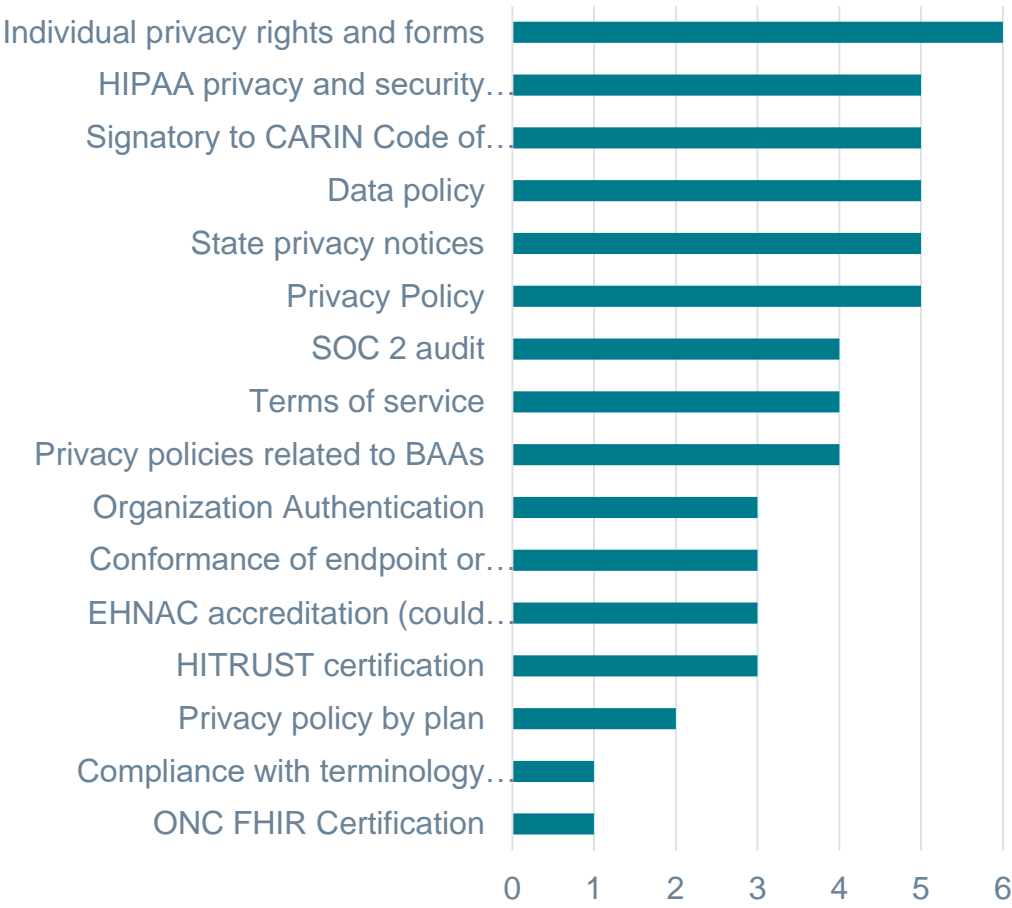
☐ Other

We received completed responses from 7 different organizations, which revealed areas of consensus, and areas that need further discussion

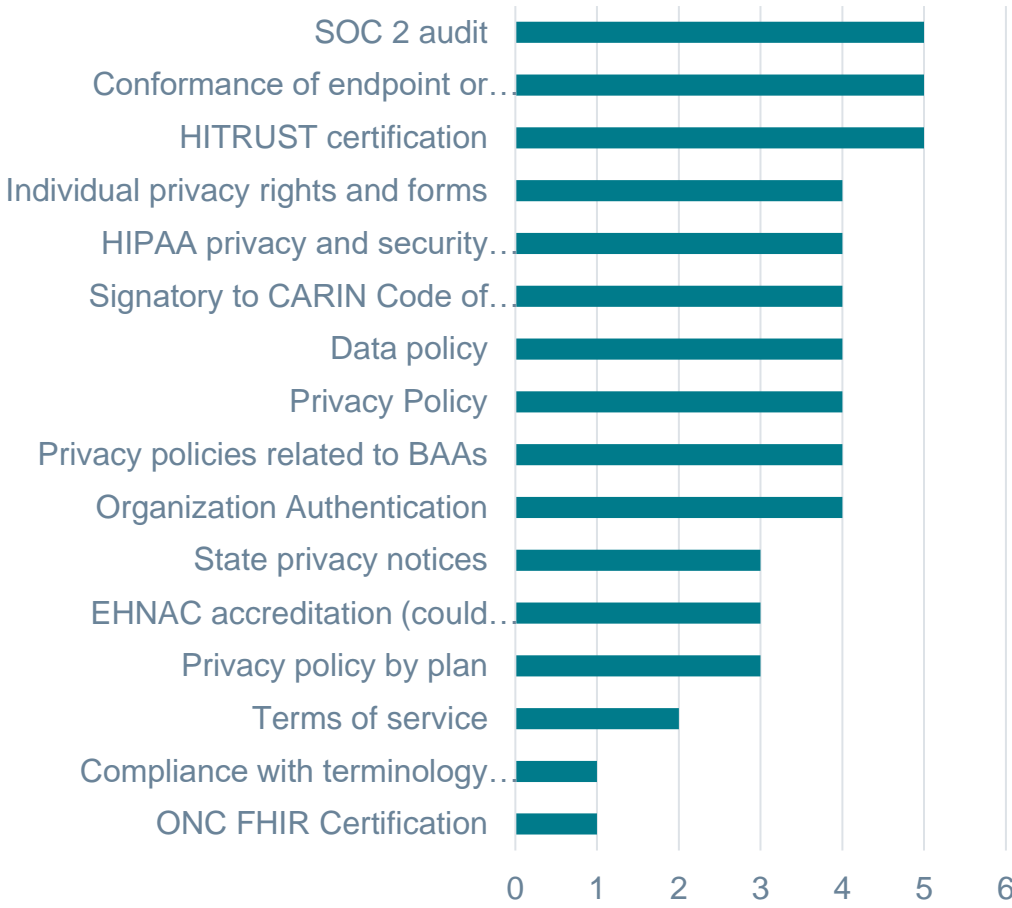
Areas of Consensus		Areas for Discussion	
			
Topic 1: Privacy, Security and Data Policies, Provisions & Attestations	<ul style="list-style-type: none">Important documents/ attestation items	<div><ul style="list-style-type: none">Document upload vs. attestation questionCritical elements of each item</div>	Today's focus
Topic 2: Conformance Testing	<ul style="list-style-type: none">Critical tests to perform	<div><ul style="list-style-type: none">Breadth and depth of testing</div>	Next session
Topic 3: Revalidation Cadence	<ul style="list-style-type: none">Revalidation cadence	N/A	
Topic 4: Health Plan Identifiers & Endpoint Organizational Hierarchy	<ul style="list-style-type: none">Top of endpoint hierarchyNo need-to-know intermediary	<div><ul style="list-style-type: none">Details around resolving information to correct endpoint</div>	Today's focus
Topic 5: Overall Rating	<ul style="list-style-type: none">Importance of seeing an organization's rating	<div><ul style="list-style-type: none">Details around scoring mechanism/rules</div>	Next session

Topic 1 Results: Privacy, Security, and Data Policies, Provisions, and Attestations

A) It is important for organizations to upload a document or provide a URL in support of this item.



B) It would be helpful to have organizations answer questions about this item on a standard attestation questionnaire.



Topic 2 Results: Conformance Testing



Most respondents would like to see the following **tests completed by a third-party app vendor**:

- Connectivity and security test (test connection using dummy client ID/secret key, etc.)
- Patient Access API test (successful and conformant query and display of response)
- Provider Directory API test (successful and conformant query and display of response)

Additional Test Suggestions

- Formulary Test
- CARIN test suite compliance
- Connectivity, security, performance and provide stress testing results



Most respondents would like to see the following **tests completed by payers**:

- Connectivity and security (test connection using dummy client ID/secret key, etc.)
- Basic endpoint status test (test that a payer's API is available)

Topic will be revisited during the 12/1/20 Work Group session

Other Tests to Revisit

- Provider Directory API test (successful and conformant query and response)
- Patient Access API test (successful and conformant query and response)

Topic 3 Results: Revalidation Cadence

Revalidation of Privacy, Security, and Data Use Information



Most respondents want **third-party app vendors & payers** to **revalidate that the information they provided related to privacy, security, and data use** is still accurate based on the following cadence:

- *Aligned to relevant policy/provision updates, but if no updates occur within a year, prompt organization for revalidation.*

Revalidation of Conformance Testing



Most respondents want **payers** to **revalidate their endpoint's conformance testing** based on the following cadence:

- *Aligned to endpoint updates, but if no updates occur within a year, prompt organization for revalidation.*

Most respondents indicated that **third-party apps** should revalidate their **app's conformance testing** based on the following cadence:

- *Aligned to app version updates, but if no updates occur within a year, prompt organization for revalidation.*
- *Note: Slightly more variation in this response than others (e.g. revalidation based on app updates only).*

Topic 4 Results: Health Plan Identifiers and Endpoint Organizational Hierarchy



Most respondents have **endpoints organized by:**

- Payer/Carrier
- Line of Business (LOB)
- Functional Department (e.g. claims system, provider network, etc.)
- Use Case

Note

When asked to order the above items in terms of information hierarchy for endpoint organization, respondents listed the following order: payer/carrier, LOB, use case, and functional department. However, fewer organizations responded to this question.

Most respondents indicated that the following **organization IDs** are necessary (for third-party apps and other payers) to identify and query payers in the directory:

- Federal Tax Identification Number (TIN/EIN)
- Health Plan/Trading Partner ID

Comments

- “Consider a CAQH ID”

Other Endpoint Organization Characteristics

- Payer (Health Plan) versus Provider (Clinical)



There was **no clear consensus** to the question: “As a responding payer, would you consider using Member ID, Group ID, or other information on a member’s insurance card to resolve to the correct Endpoint?”

Comments

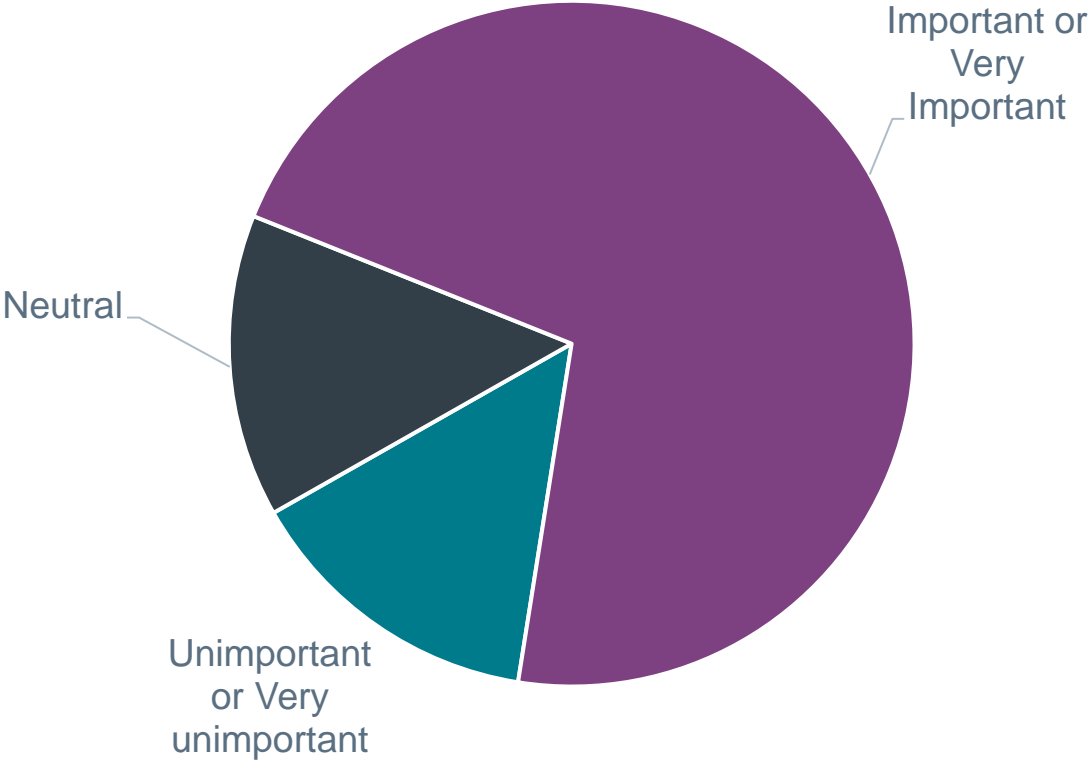
- “Seems problematic since these IDs are not coordinated across organizations”

Most respondents were **neutral** when asked: “How important is it to know or represent that an endpoint is operated by an intermediary?”

Topic 5 Results: Additional Feedback – Importance of Showing a Rating

How important is it to your organization to be able to see an overall rating that indicates how organizations scored in areas related to privacy, security, and data use, and conformance testing?

Most respondents felt it was **important or very important** to be able to **see an overall rating** that indicates how organizations scored in areas related to privacy, security, and data use, and conformance testing.



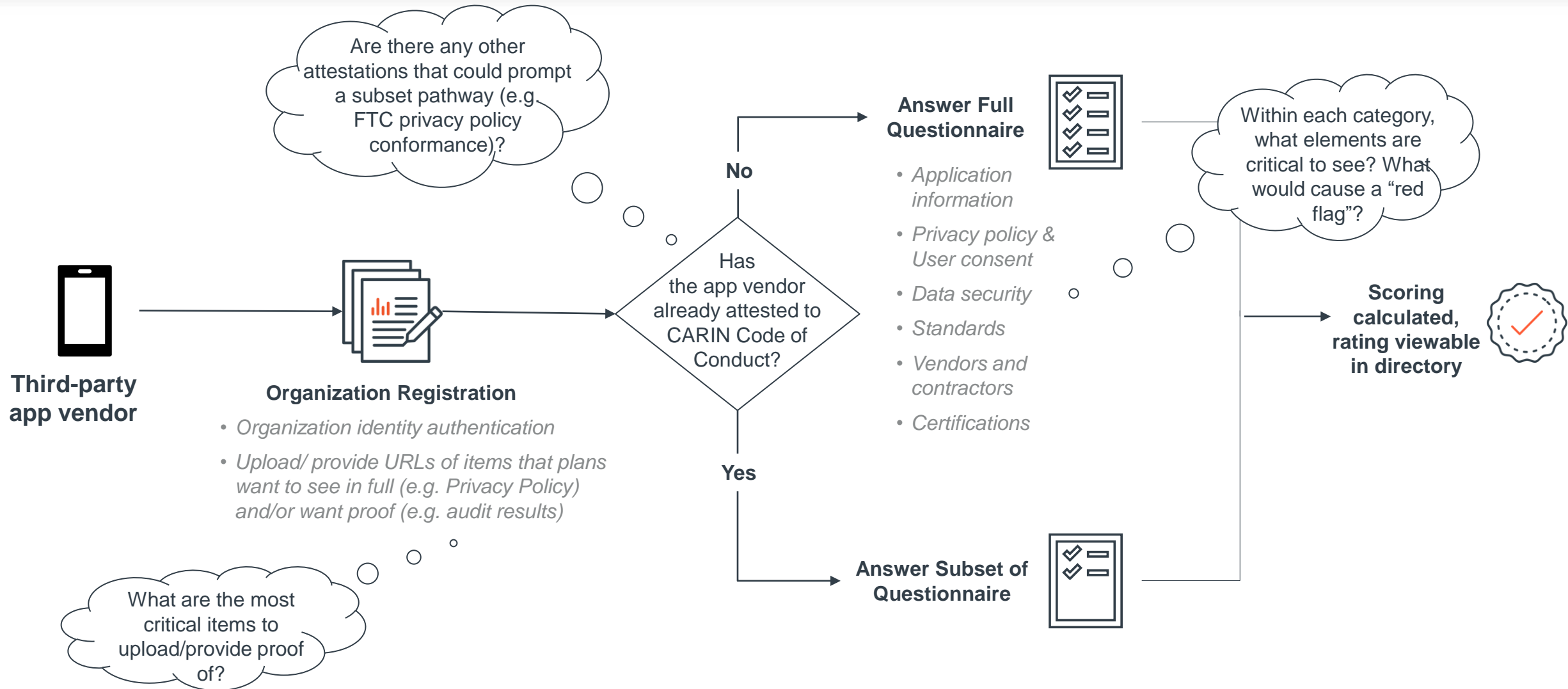
Topic will be revisited during the 12/1/20 Work Group session

Time (ET)	Topic
3:00-3:10pm	Welcome
3:10-3:35pm	Straw Poll Results
3:35-4:10pm	Discussion: Topic #1 – Privacy, Security and Data Policies, Provisions & Attestations
4:10-4:40pm	Discussion: Topic #4 – Endpoint Hierarchy & Org IDs
4:40-4:50pm	Looking Ahead
4:50-5:00pm	Next Steps

Discussion: Privacy, Security and Data Policies, Provisions & Attestations

- Consensus areas:
 - Items that are important to collect information on, in general, pertain to the following categories:
 - Privacy policy (including individual privacy rights),
 - Security (can include SOC 2 audit, HIPAA privacy and security compliance, data security, etc.),
 - Data use policy, and
 - Overall attestation to industry code of conduct (e.g. CARIN Code of Conduct).
- For further discussion:
 - Can we assume that the items lower on the list are not as important to collect information about?
 - Which of these items truly need a document upload?
 - Which elements within these items do privacy officers within your organization look for?
 - Do the results signal which items should be valued higher for a rating system?
 - Isolate which items differ for payers vs. third-party apps.

Discussion: Privacy, Security and Data Policies, Provisions & Attestations



Within each category, what elements are critical to about a third-party app vendor?

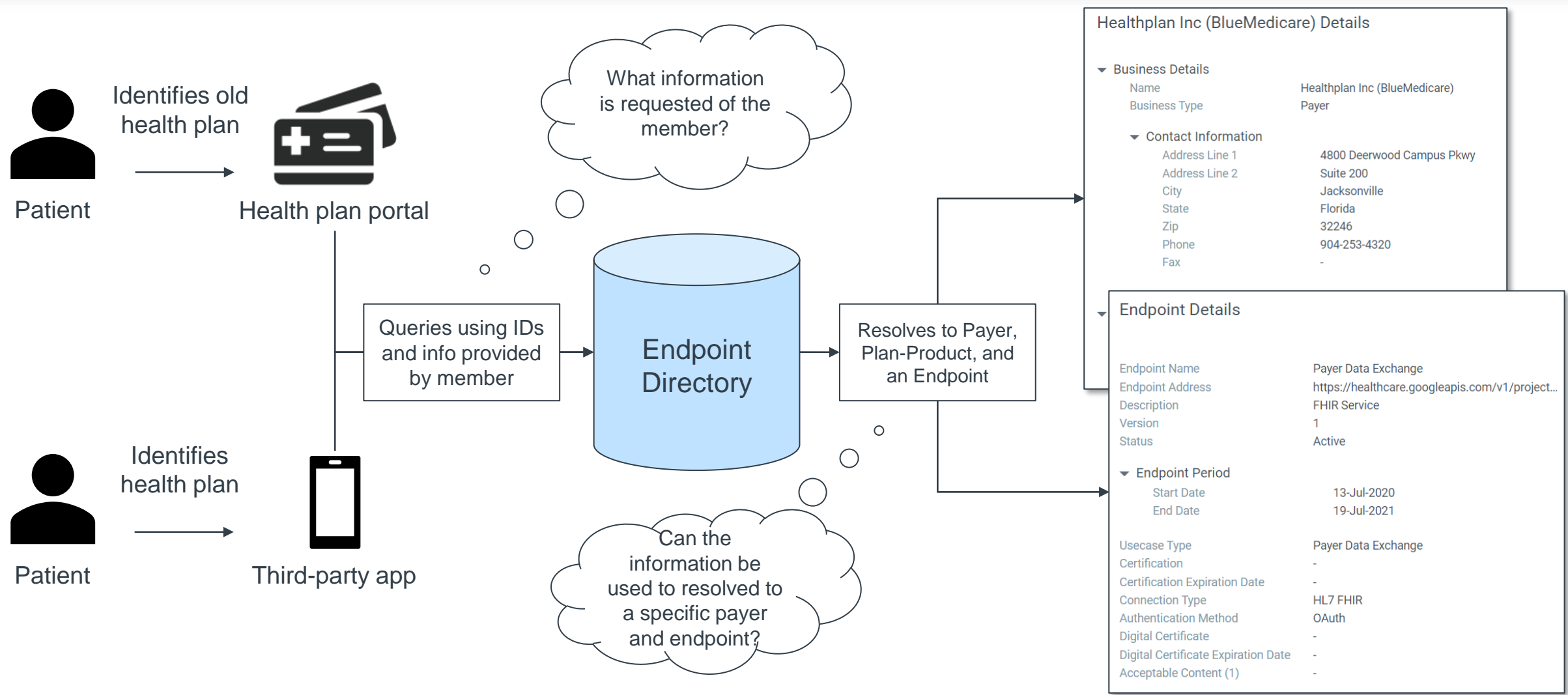
Category		Question Topics – <i>Not Exhaustive</i>	Notes <ul style="list-style-type: none">• Questions/ topics draw heavily from CARIN Code of Conduct• Organization identity authentication will happen prior to Questionnaire• May be slight differences between necessary items for payer vs. third-party app vendor
1	Application Information	<ul style="list-style-type: none">▪ 1.1 Number of users▪ 1.2 Application status (released for public use?)	
2	Privacy Policy & User Consent	<ul style="list-style-type: none">▪ 2.1 Details on individual privacy rights and forms▪ 2.2 State privacy notices▪ 2.3 Privacy policy by plan▪ 2.4 General user readability, explanation of risks▪ 2.5 Terms of use▪ 2.6 General data use▪ 2.7 Secondary data uses and/or sharing▪ 2.8 Notification, consent▪ 2.9 Data retention and data use if user has withdrawn consent▪ 3.0 Compliance with HIPAA privacy and security; Federal Trade Commission privacy policy	
3	Data Security	<ul style="list-style-type: none">▪ 3.1 Data storage (what, where, how)▪ 3.2 Data encryption (for both data at rest and data in motion)▪ 3.3 Data deletion (soft vs hard; handling data stored on backup)▪ 3.4 Data access; minimizing risk of unauthorized access/use	
4	Standards	<ul style="list-style-type: none">▪ 4.1 Indication of conformance of endpoint or application with FHIR and RESTful standards (e.g. ONC FHIR certification, etc.)▪ 4.2 Indication of compliance with terminology licensing requirements (e.g., AMA, AHA, X12, etc.).	
5	Vendors and Contractors	<ul style="list-style-type: none">▪ 5.1 Assurance that any vendors/contractors comply with third party app's privacy policy, terms of service, data security and sharing practices	
6	Certificates/ Accreditations	<ul style="list-style-type: none">▪ 6.1 Opportunity to indicate if the third-party app vendor has any certifications or of note that signal trustworthiness (e.g. SOC 2 audit, HITRUST certification, EHNAC accreditation, etc.)	

Time (ET)	Topic
3:00-3:10pm	Welcome
3:10-3:35pm	Straw Poll Results
3:35-4:10pm	Discussion: Topic #1 – Privacy, Security and Data Policies, Provisions & Attestations
4:10-4:40pm	Discussion: Topic #4 – Endpoint Hierarchy & Org IDs
4:40-4:50pm	Looking Ahead
4:50-5:00pm	Next Steps

Discussion: Endpoint Hierarchy & Org IDs

- Consensus areas:
 - Payer endpoints are most often organized by payer/carrier and by line-of-business.
 - Payer/carrier and line-of-business are at top of hierarchy, followed by functional department and use case.
 - TIN/EIN and clearinghouse trading partner IDs are the most cited identifiers for payers.
- For further discussion:
 - What information is expected to be provided by member to third-party apps and payers?
 - How information provided by the member can resolve to a payer ID?
 - How your organization will resolve payer IDs and other information to one of your endpoints?

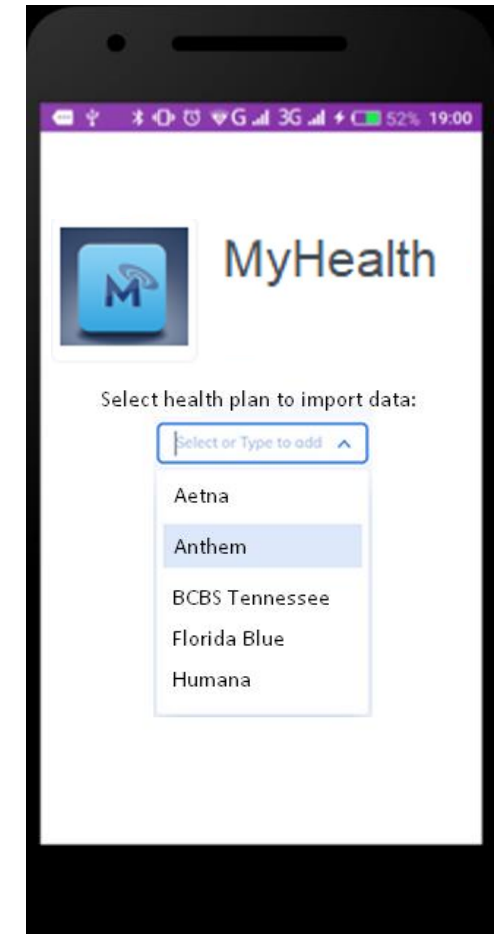
The role of payer IDs and organizational hierarchy in endpoint resolution



What information will be captured from a member to resolve to a payer endpoint?

- Survey response: Most health plans were either **uncertain** or **did not agree** that information on a member's insurance card (e.g., member ID, group ID) could be used to resolve to a payer's endpoint.
- Discussion questions:
 - As a payer, what information will you ask members about their old payer, to determine how to resolve the request to the old payer's endpoint?
 - > Is it simply the health plan name?
 - > Would you need to support all plan-product variations and LoB in a picklist that would resolve to different endpoints, or would you ask those as separate questions?
 - What information do you expect third-party apps to ask members about their payer, to determine how to resolve the request to a payer's endpoint?
 - > Is it simply the health plan name?
 - > Would you need to support all plan-product variations and LoB in a picklist that would resolve to different endpoints, or would you ask those as separate questions?
 - What exception processes initiate when the member does not know?
 - How will information collected from a member resolve to a specific payer ID?

**Illustrative wireframe
for discussion:**



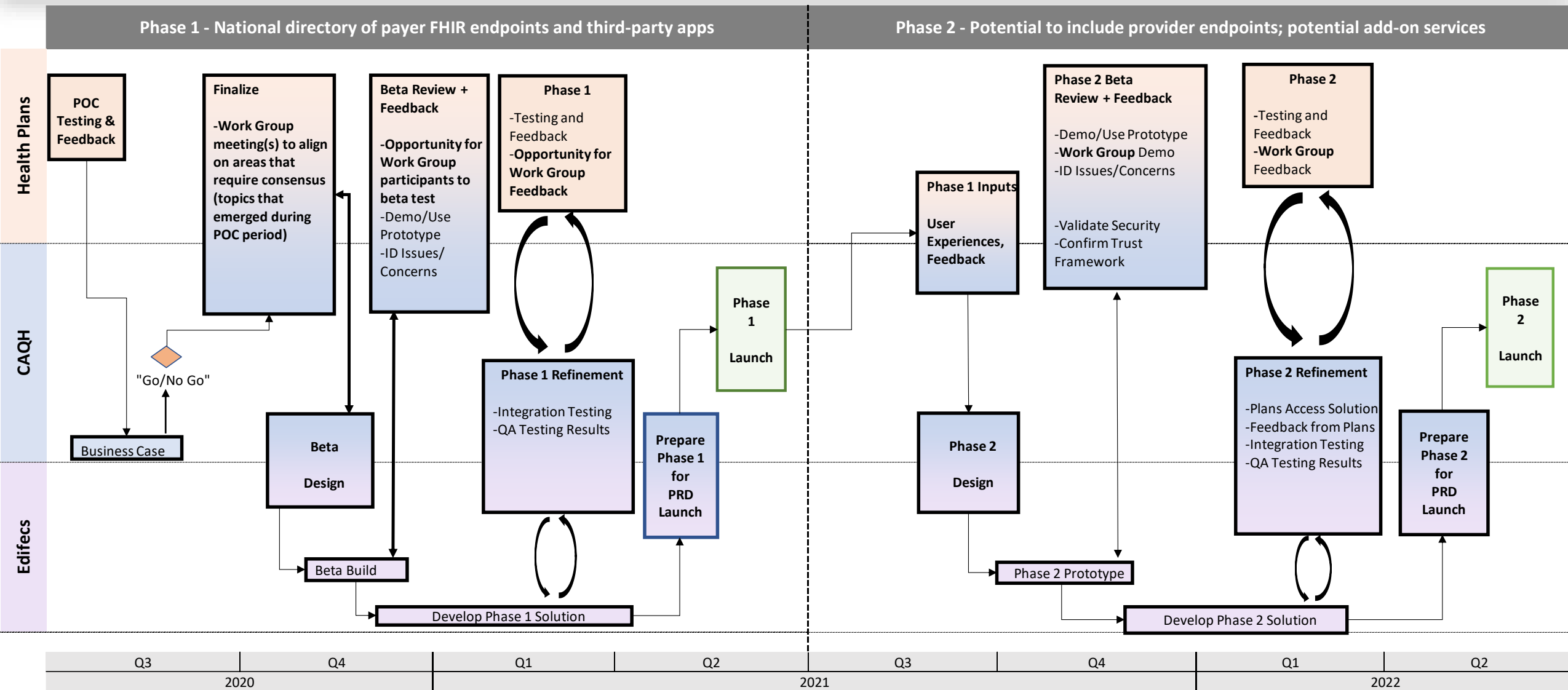
How can payer ID and other information be used to resolve to a payer's endpoint?

- Survey responses:
 - Payer endpoints are most often organized by payer/carrier and by line-of-business.
 - Payer/carrier and line-of-business are at top of hierarchy, followed by plan-product and use case.
 - TIN/EIN and clearinghouse trading partner IDs are the most cited identifiers for payers.
- Discussion questions:
 - As a responding payer, what combination of search criteria would need to be used by third-party apps and other payers to resolve to a single endpoint that could be called against? Examples:
 - > Payer/carrier and line-of-business
 - > Payer/carrier and Payer ID
 - > Payer/carrier and trading partner ID
 - > Payer/carrier and use case
 - > Payer/carrier, plan-product, and trading partner ID
 - As a responding payer, to what extent will you have a single endpoint that utilizes other information that the member has provided to automatically locate or route the request to the proper 'responding system'?
 - As a requesting payer, what information will you have on hand to resolve to another payer's endpoint?

Time (ET)	Topic
3:00-3:10pm	Welcome
3:10-3:35pm	Straw Poll Results
3:35-4:10pm	Discussion: Topic #1 – Privacy, Security and Data Policies, Provisions & Attestations
4:10-4:40pm	Discussion: Topic #4 – Endpoint Hierarchy & Org IDs
4:40-4:50pm	Looking Ahead
4:50-5:00pm	Next Steps

Roadmap

Beta Launch Q4 2020, Phase 1 Full Launch Q2 2021



Looking ahead – remaining sessions

Session	Date/Time	Topics
---------	-----------	--------

*Following today’s session (Session #2), your organization will review **the Draft Standard Questionnaire** and will provide live feedback during Session #3.*

Session #3	Tuesday, 12/01/20	<ul style="list-style-type: none">▪ Review participants’ feedback on privacy/security questionnaire▪ Discuss breadth and depth of testing▪ Begin discussing rubric/scoring
	12:30-2:30pm ET	
Session #4	Friday, 12/11/20	<ul style="list-style-type: none">▪ Continue discussion of rubric/scoring mechanism▪ Finish discussion of any remaining items
	3:00-5:00pm ET	

*Opportunity for continued detailed feedback via **Beta Testing** in late December/January.*

Opportunity to participate in beta testing

CAQH is recruiting health plans and third-party app vendors to beta test the Endpoint Directory and Third-Party App Registry.



Timing: Begins in mid-Dec. 2020 and runs through Jan. 2021.



Scope:

- Payer org and endpoint data input into directory.
- Payer review of third-party app information.
- Payer query for other payers' endpoints.
- Connection requests.



Expectations:

- Intent for production commitment.
- Feedback on ease of use, completeness of solution.
- Timely completion of beta test scenarios.
- Feedback on level of automation possible.
- Reporting on success of specific test scenarios.

Time (ET)	Topic
3:00-3:10pm	Welcome
3:10-3:35pm	Straw Poll Results
3:35-4:10pm	Discussion: Topic #1 – Privacy, Security and Data Policies, Provisions & Attestations
4:10-4:40pm	Discussion: Topic #4 – Endpoint Hierarchy & Org IDs
4:40-4:50pm	Looking Ahead
4:50-5:00pm	Next Steps

Next Steps

1. **CAQH staff send Draft Standard Questionnaire** to work group participants.
2. **Participants review draft attestation questionnaire**; come ready to discuss next session.
3. **Participants discuss Beta Testing opportunity with their organization.**
4. **Attend remaining sessions:**

Tuesday, 12/1/20, 12:30-2:30pm ET

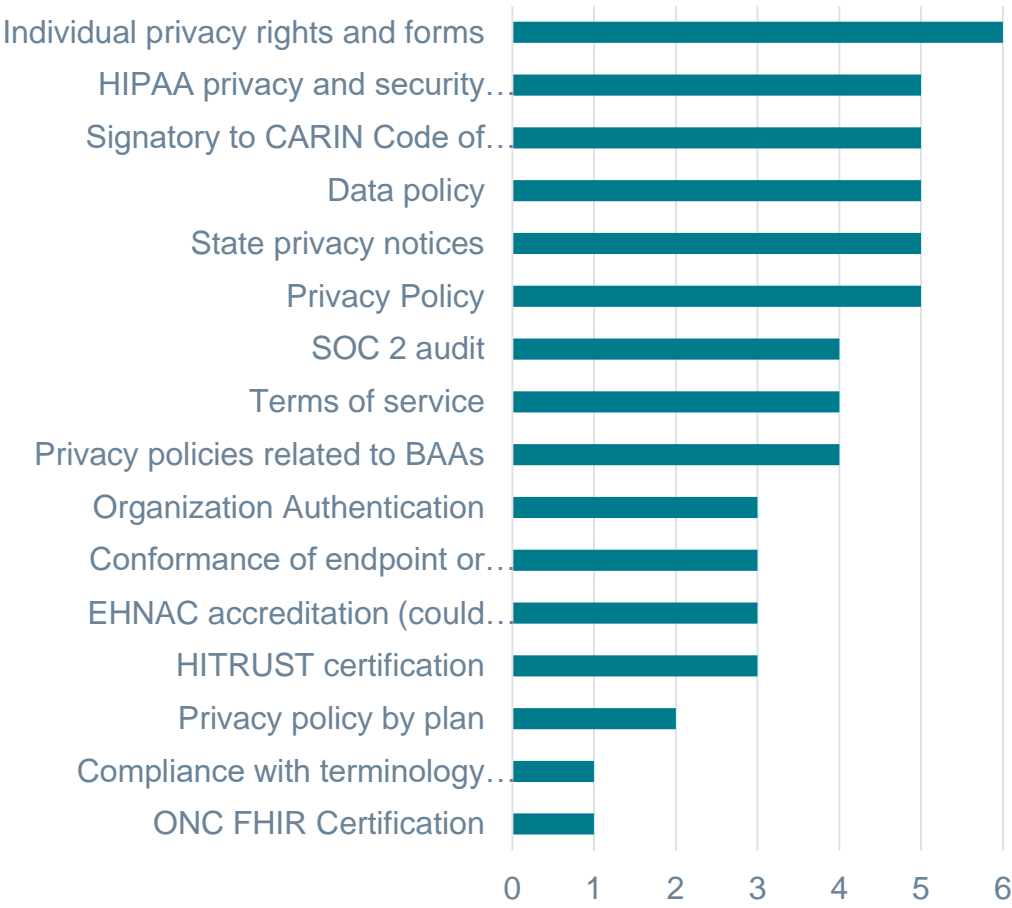
Friday, 12/11/20, 3:00-5:00pm ET

APPENDIX

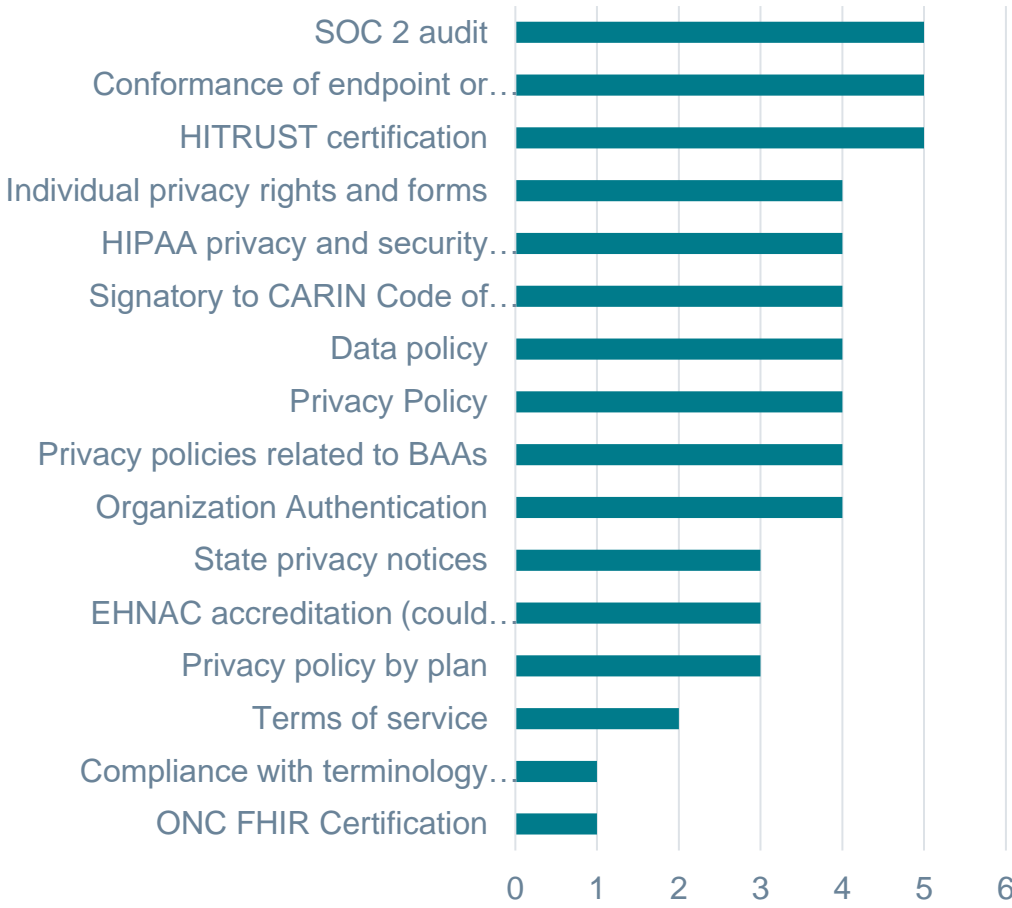
Detailed Results

Topic 1 Results: Privacy, Security, and Data Policies, Provisions, and Attestations

A) It is important for organizations to upload a document or provide a URL in support of this item.



B) It would be helpful to have organizations answer questions about this item on a standard attestation questionnaire.



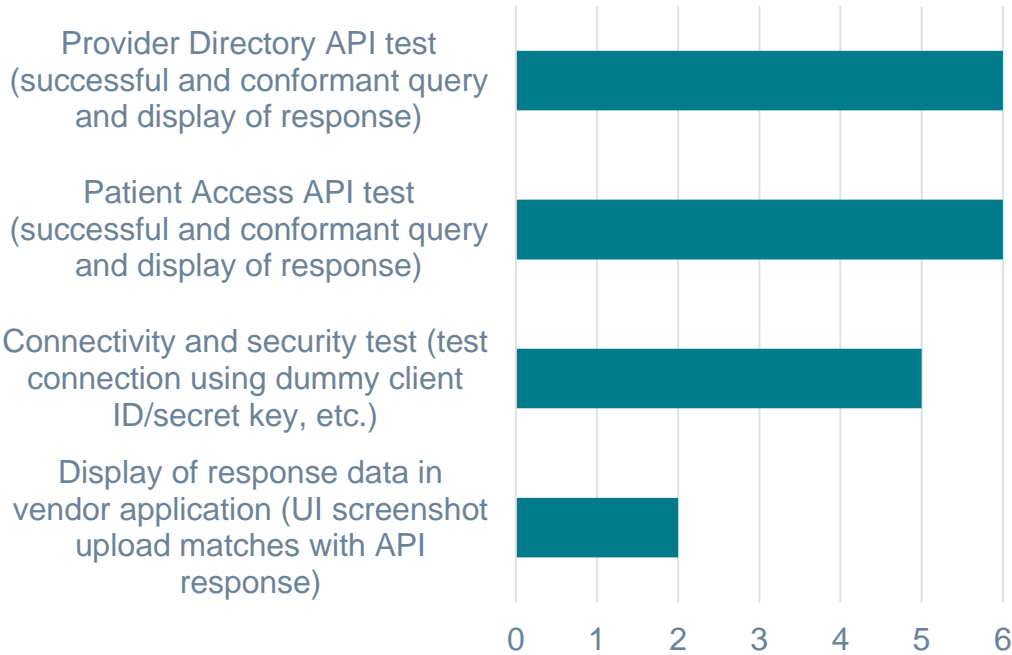
Topic 1 Results: Privacy, Security, and Data Policies, Provisions, and Attestations

Of the items listed above, please list the 10 that are highest priority for your organization to see about another organization (payer or third-party app), with 1 being the top priority.		Rank
<i>High Priority</i>	Privacy Policy	1
	Individual privacy rights and forms	2
	Signatory to CARIN Code of Conduct	3
	Conformance of endpoint or application with FHIR and RESTful standards	4
	Organization Authentication	5
<i>Medium Priority</i>	Data policy	6
	Terms of service	7 (tie)
	HIPAA privacy and security compliance	7 (tie)
	Privacy policies related to BAAs	9
	SOC 2 audit	10
<i>Low Priority</i>	HITRUST certification	11
	State privacy notices	12 (tie)
	EHNAC accreditation (could include EHNAC/UDAP "Trusted Dynamic Registration & Authentication Accreditation Program)	12 (tie)
	Privacy policy by plan	14
	Compliance with terminology licensing requirements (e.g., AMA, AHA, X12)	15
	ONC FHIR Certification	16

Due to low response rate, we'll be **revisiting this question** in the discussion section

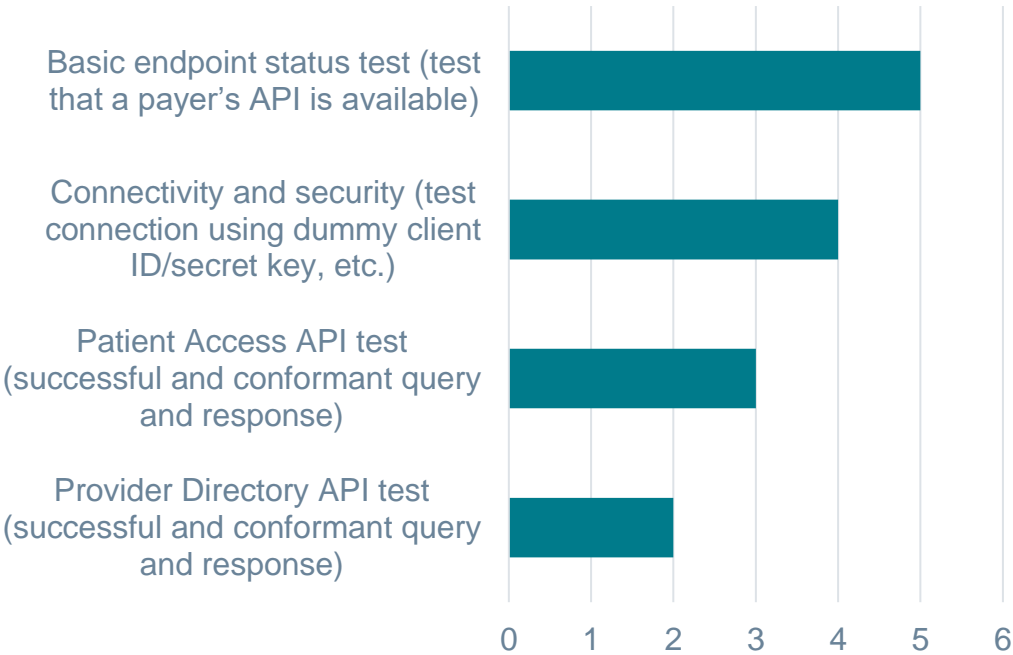
Topic 2 Results: Conformance Testing

At a high-level, which of the following tests would you like to see completed by a **third-party app vendor**:



Comments
<ul style="list-style-type: none">• Formulary Test• CARIN test suite compliance• Connectivity, security, performance and provide stress testing results

At a high-level, which of the following tests would you like to see completed by other **payers**:

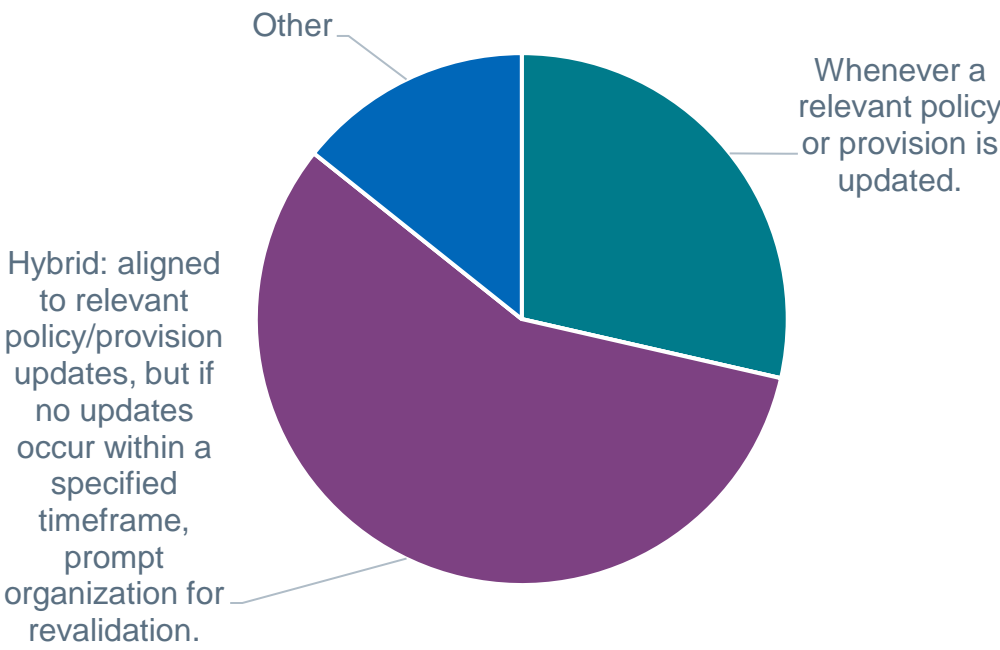


Comments
<ul style="list-style-type: none">• Payer-to-payer

Topic will be revisited during the 12/1/20 Work Group session

Topic 3 Results: Revalidation Cadence for Privacy, Security & Data Use Information

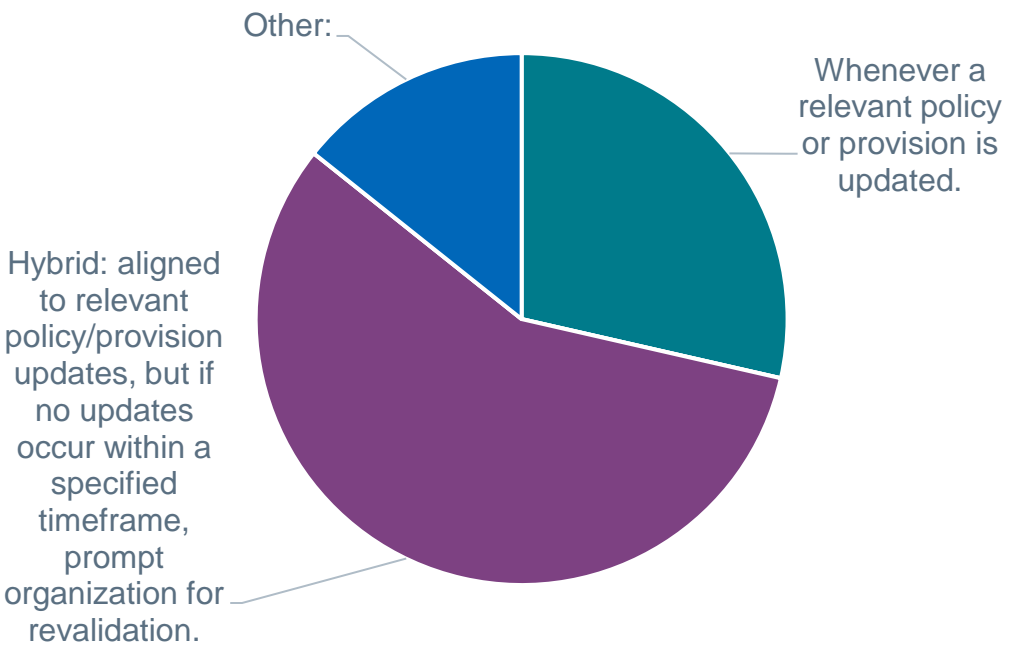
At what cadence would you like to see **third-party app vendors** be prompted to revalidate that the information they provided related to privacy, security, and data use is still accurate and current?



Comments

“We generally take a risk-based approach depending on our confidence and experience with the Partner’s handling of PHI”

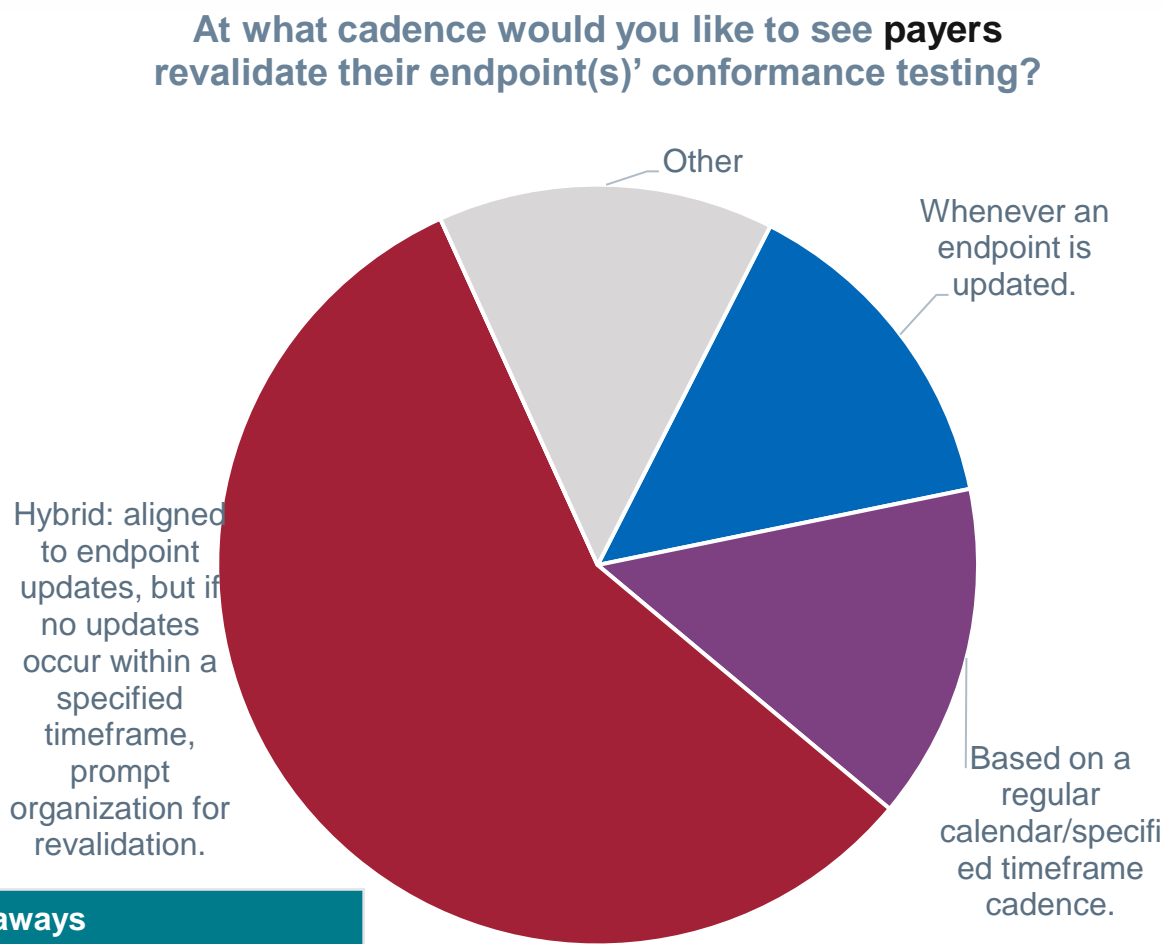
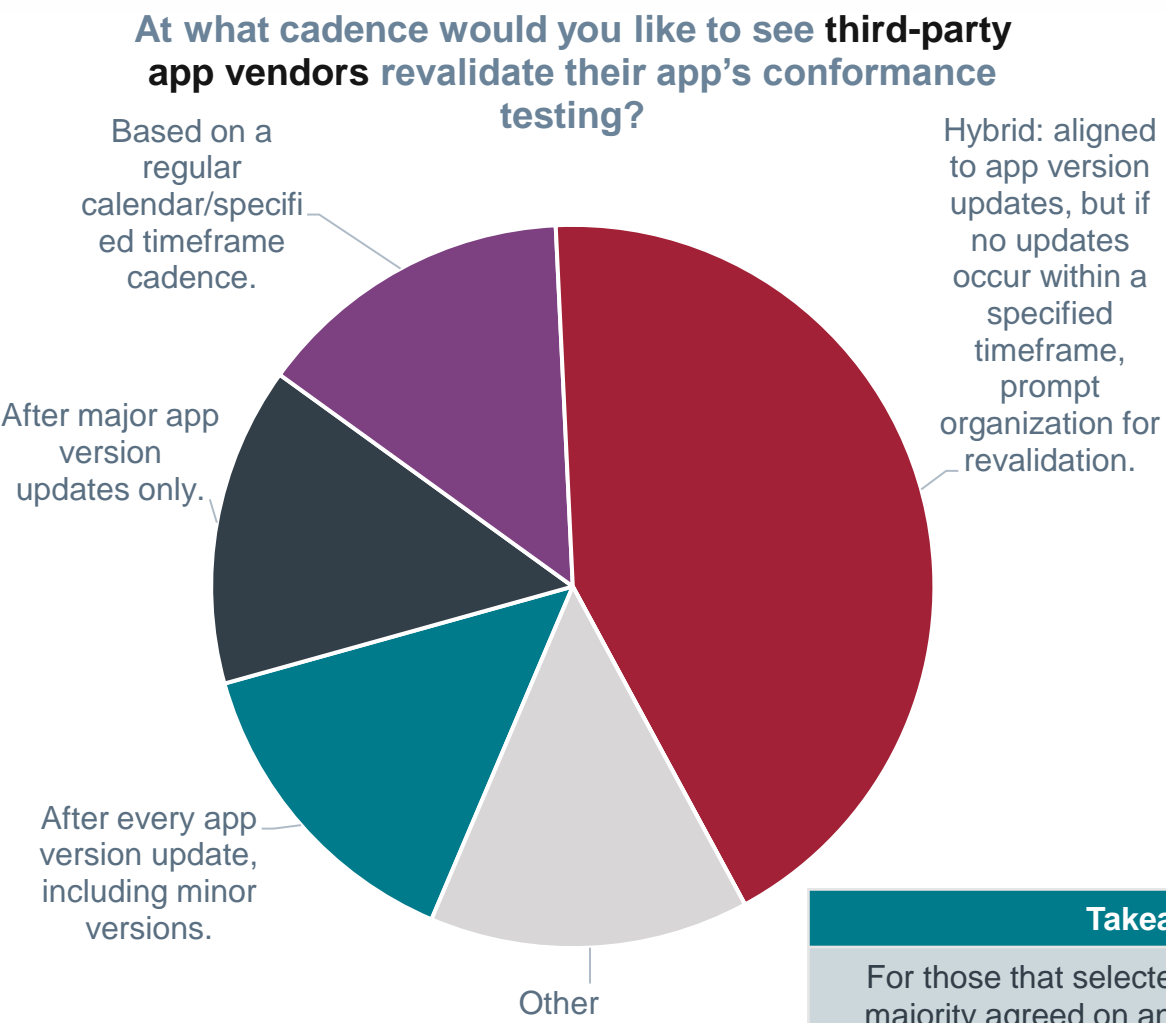
At what cadence would you like to see **payers** be prompted to revalidate that the information they provided related to privacy, security, and data use is still accurate and current?



Takeaways

For those that selected a hybrid model, the majority agreed on an **annual revalidation cadence** for vendors and payers

Topic 3 Results: Revalidation Cadence for Conformance Testing

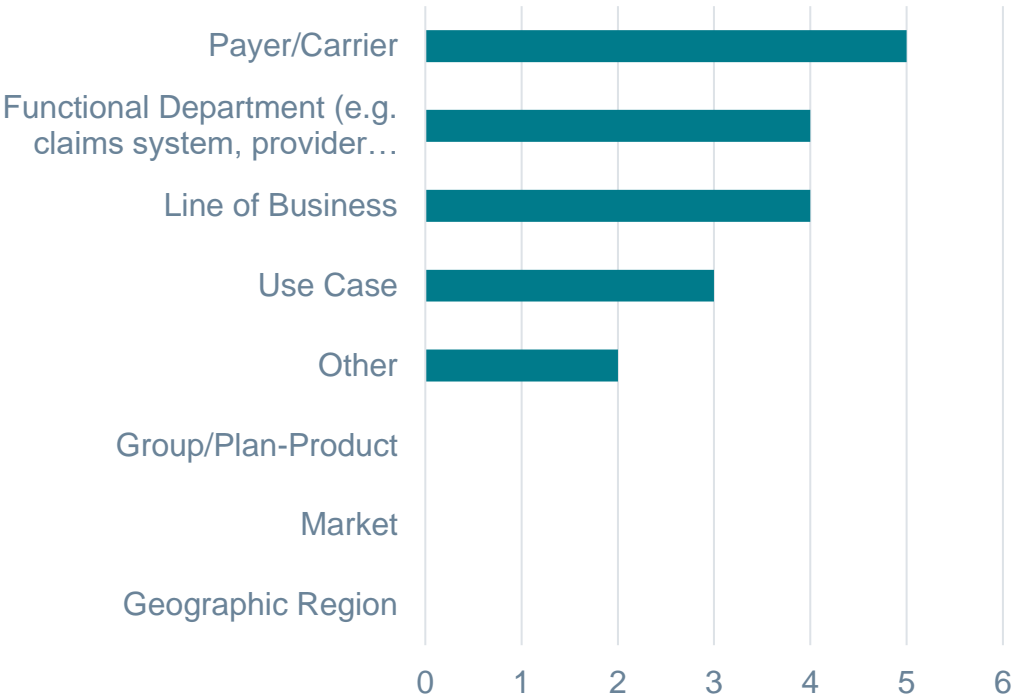


Takeaways

For those that selected a hybrid model, the majority agreed on an **annual revalidation cadence** for vendors and payers

Topic 4 Results: Health Plan Identifiers and Endpoint Organizational Hierarchy

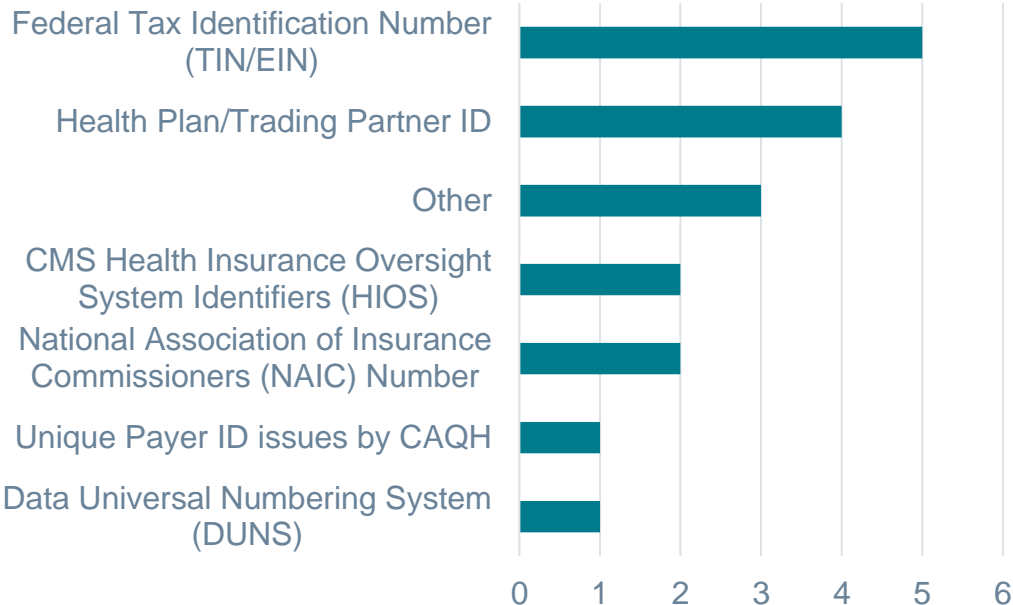
By which characteristic are your endpoints organized? Select all that apply.



Comments

- Payer(Health Plan) versus Provider (Clinical)

Which organization IDs are necessary (for third-party apps and other payers) to identify and query payers in the directory? Select all that apply.

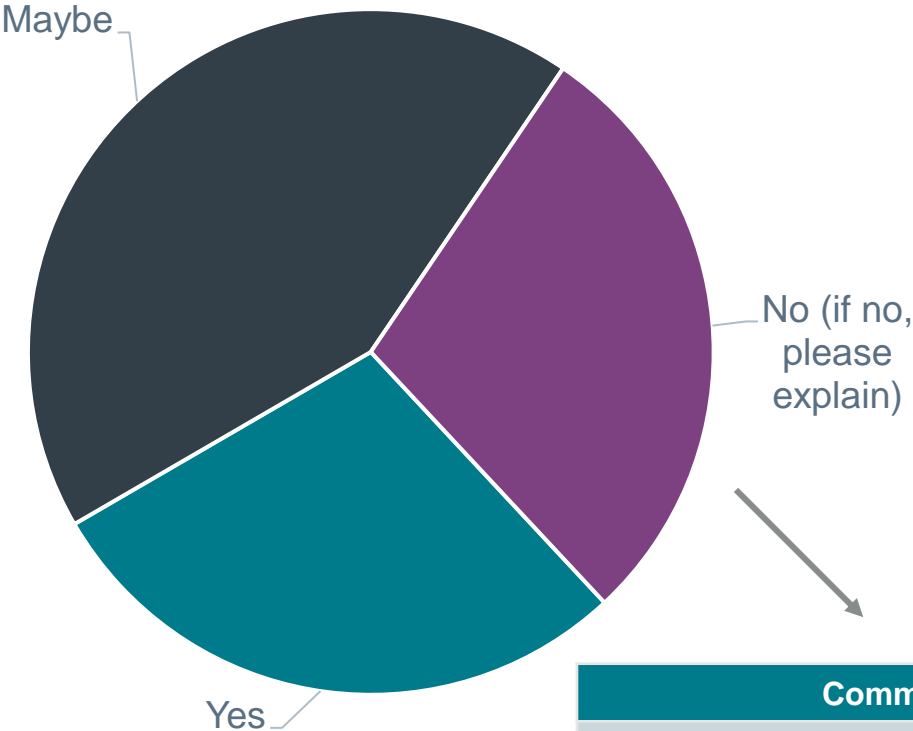


Comments

- Unique Payer ID issued by CAQH

Topic 4 Results: Health Plan Identifiers and Endpoint Organizational Hierarchy

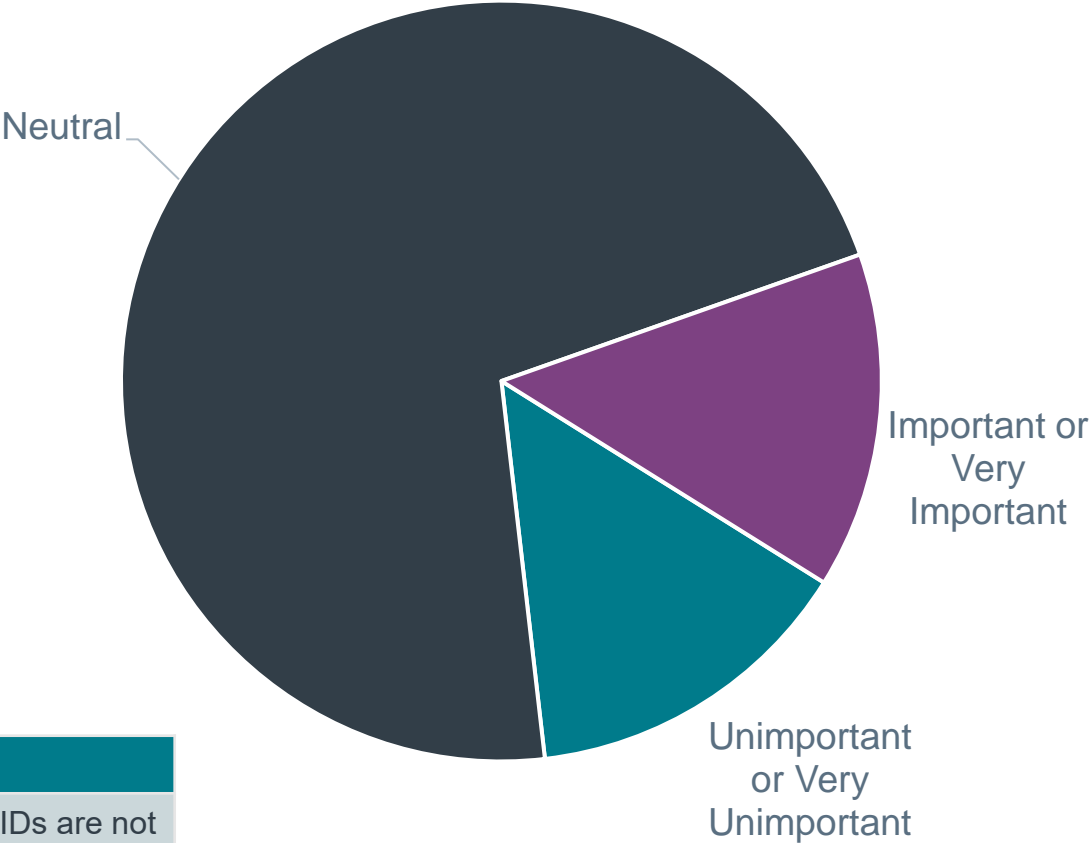
Plan Resolution: As a responding payer, would you consider using Member ID, Group ID, or other information on a member’s insurance card to resolve to the correct Endpoint?



Comments

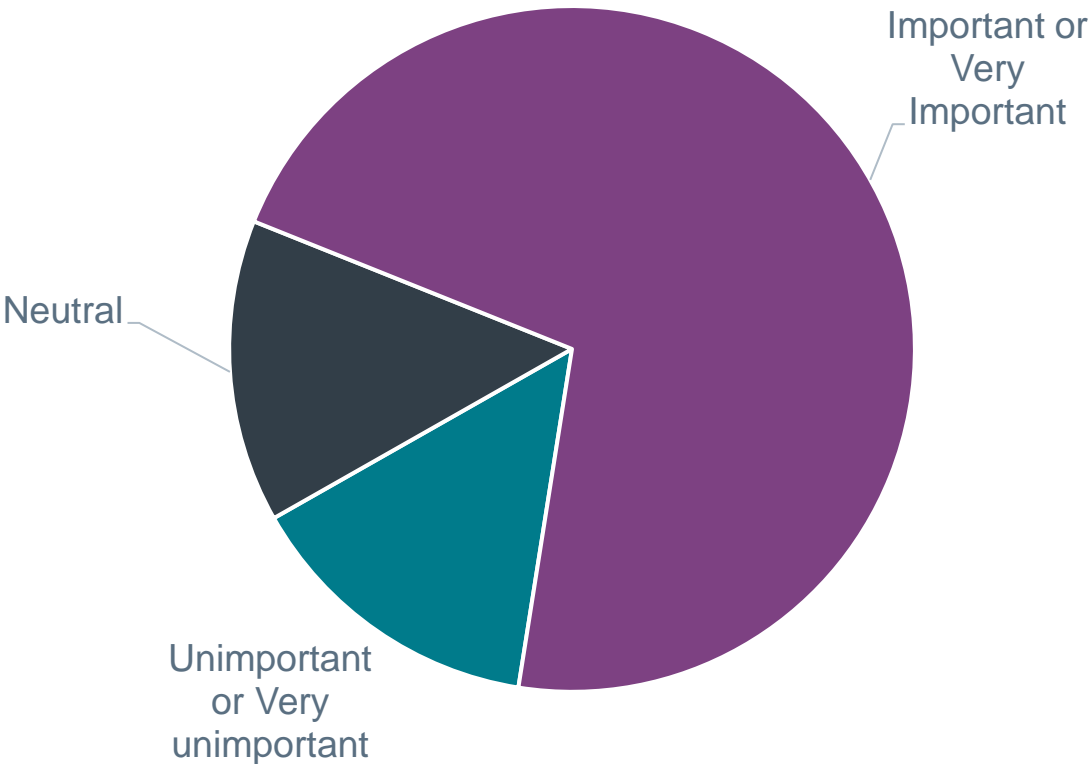
“Seems problematic since these IDs are not coordinated across organizations.”

How important is it to know or represent that an endpoint is operated by an intermediary?



Topic 5 Results: Additional Feedback – Overall Rating for Organizations

How important is it to your organization to be able to see an overall rating that indicates how organizations scored in areas related to privacy, security, and data use, and conformance testing?



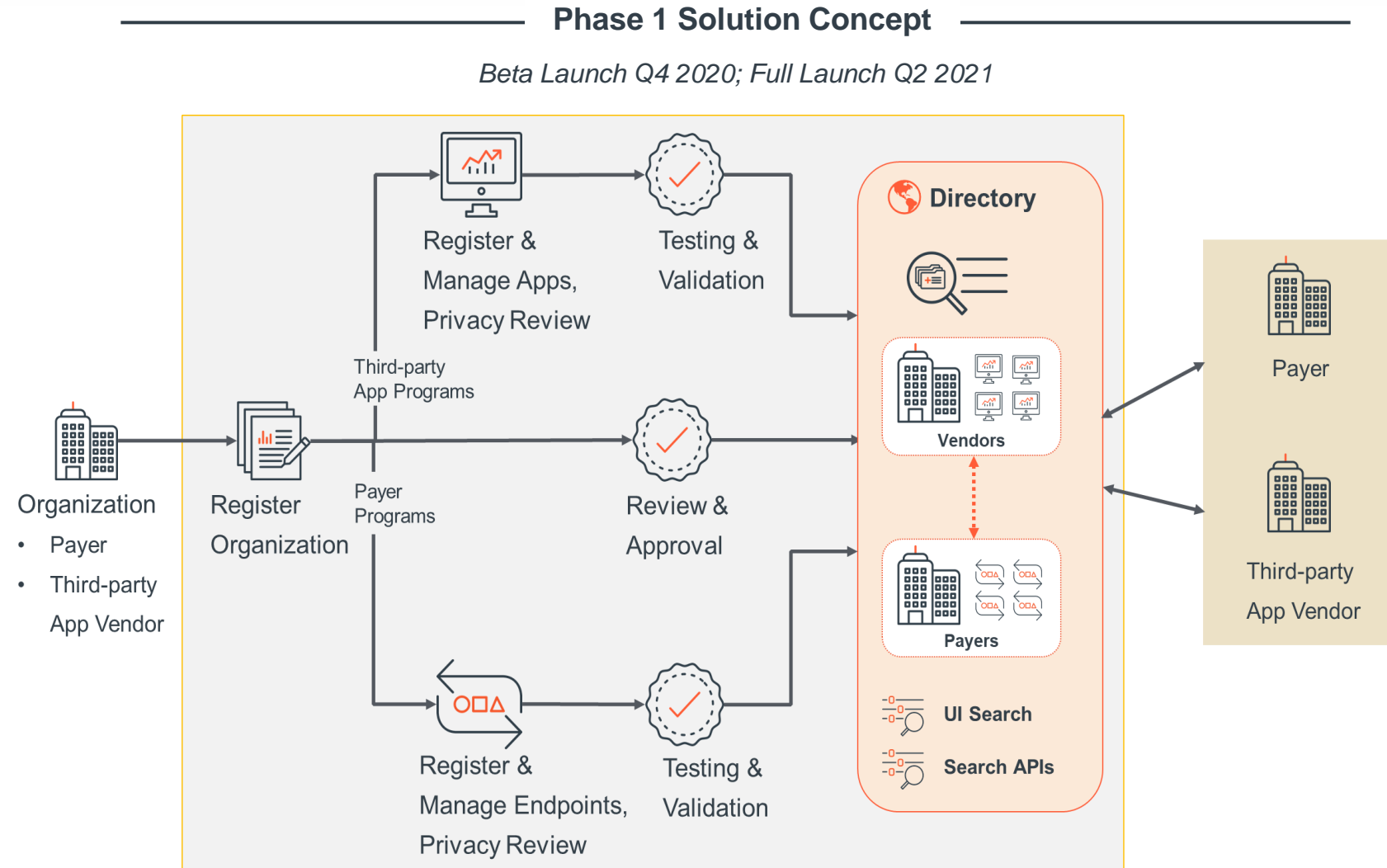
Topic will be revisited during the 12/1/20 Work Group session

Solution Scope

Solution Concept: A National Utility for Payer Endpoints & Third-party App Registry

A national source of truth for validated payer endpoints and third-party apps that:

- Allows payers to **share information about endpoints**, including capability statement imports. Simplifies, automates manual processes.
- Allows payers and third-party apps to **query payer endpoints** for multiple use cases.
- **Validates identity** of payer and third-party app participants.
- **Facilitates connection request** between parties.
- **Confirms privacy and security attestations** and/or privacy policy, data use agreements.
- **Ensures conformance testing and validation** of FHIR endpoints and ability to work with endpoints.
- Allows **third-party apps to upload information about themselves** to make available to payers.



Items that are out of scope; items that could be potential for Phase 2 scope

Out of Scope

- Obtaining patient authorization/ consent
- Issuing of client IDs and secret keys
- Routing capabilities
- Conduit of patient data between payers or between payers and third-party apps

Potential Phase 2 Scope

- Phase 2, which would beta launch Q4 2021 and fully launch Q2 2022, could include the following:
 - Provider endpoints
 - A more formalized trust framework
 - Automated client-server request/ credential check
 - Potential support for UDAP Dynamic Client Registration
 - Add-on optional services to support accurate patient matching and identification of prior coverage

Work Group & Call Information

Today's Call Documents

Document Name

CAQH Endpoint Directory Work Group_Session 2 Deck_20201113

CAQH Staff	Email Address
April Todd <i>Senior Vice President, CORE & Explorations</i>	atodd@caqh.org
Ron Urwongse <i>Director, Strategy & Innovation</i>	rurwongse@caqh.org
Rachel Goldstein <i>Senior Manager, CORE</i>	rgoldstein@caqh.org
Justin Edelman <i>Manager, Strategy & Innovation</i>	JEdelman@caqh.org
Dasia Rogers <i>Program Assistant, Solutions – Technology & Product</i>	drogers@caqh.org

CAQH Endpoint Directory Work Group Roster (as of 11/13/20)

Health Plan	Participant Name
Aetna	Hari Viswanathan
	Shivani Patel
Anthem	Brandon Raab
	Christol Green
	Kenneth Williams
	Sam Sander
	Sarah Young
BCBS FL	Amit Shah
	Court Collins
	Heather Kennedy
BCBS KS	Kevin Jones
BCBS NC	Rajiv Malik
	Phani Cherukuri
	William Moore

Health Plan	Participant Name
CareFirst	Julie Billman
Cigna	Patrick Haren
	Paul Oates
	Sandeej Kottal
	Ashley Maples
Horizon	Siobhan Matsagas
	Jacqueline Victory
Humana	Patrick Murta
Kaiser	Bryan Matsuura
	Kevin Isbell
	Radha Murakami
United	Nick Radov
	Sagran Moodley