The Office of the National Coordinator for Health Information Technology

API Conditions of Certification (and more!)

Steve Posnack, Executive Director, Office of Technology, ONC

Two Statutory Sections Implemented Together

45 CFR Part 170.4xx and Part 171.2xx

Conditions of Certification

- **170.401 Information blocking**
- **170.402 Assurances**
- **170.403 Communications**
- **170.404 APIs (without special effort)**
- **170.405 Real world testing**
- **170.406 Attestations**
- **170.40x EHR Reporting Program**

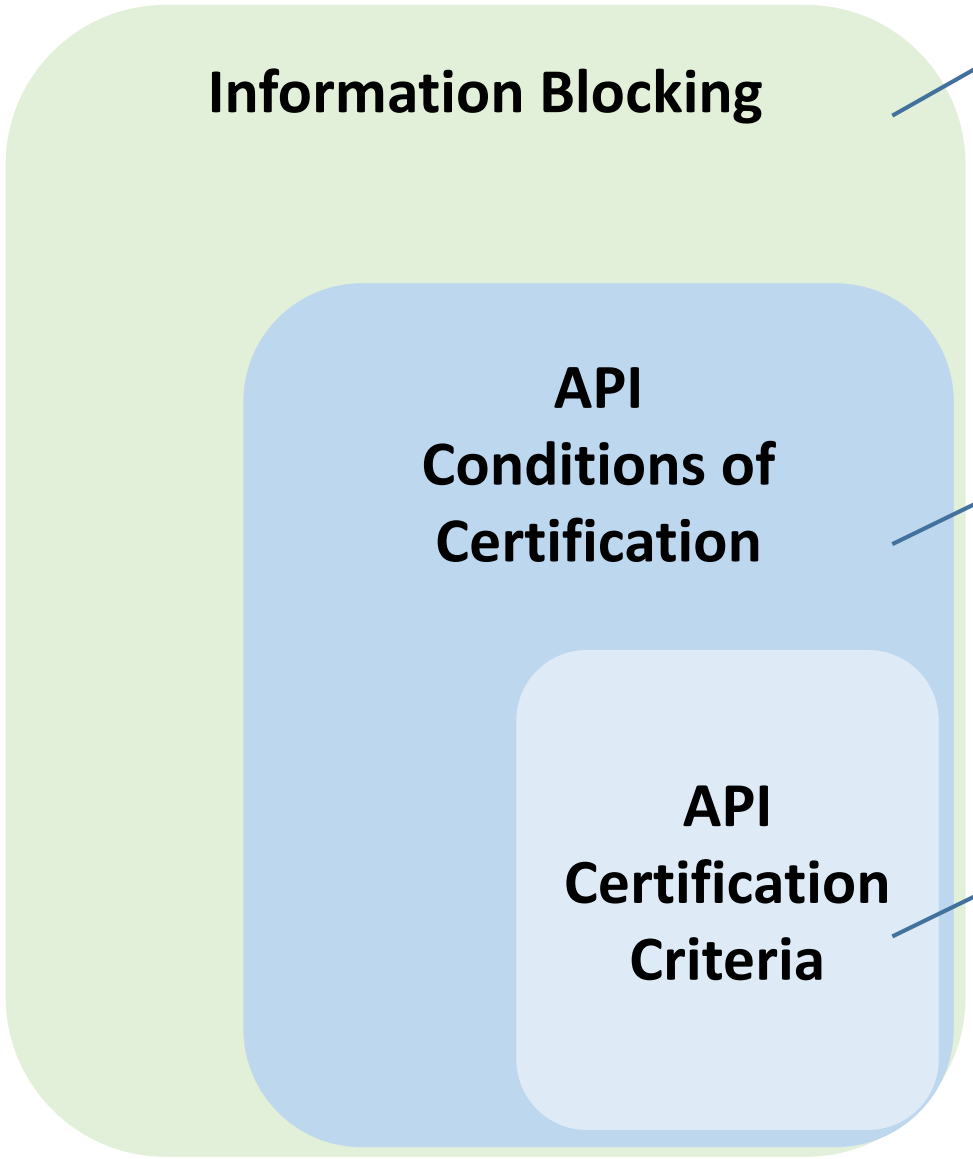
Information Blocking Exceptions

- **171.201 Preventing harm**
- **171.202 Promoting the privacy of electronic health information**
- **171.203 Promoting the security of electronic health information**
- **171.204 Recovering costs reasonably incurred**
- **171.205 Responding to requests that are infeasible**
- **171.206 Licensing of interoperability elements on reasonable and non-discriminatory terms**
- **171.207 Maintaining and improving health IT performance**

Acronym Check

- **API = Application Programming Interface**
- **FHIR® = Fast Healthcare Interoperability Resources (an HL7® standard)**
- **USCDI = United States Core Data for Interoperability**
- **ARCH = API Resource Collection in Health**

The Really Big Picture
Scope and Applicability: Certified-API Proposals



- Applies to health IT developers, health information exchanges, health information networks, and health care providers
- Electronic health information is expected to be accessible, exchangeable, & useable unless an "interference" is required by law or covered by an exception(s)
- An action(s) covered by an exception(s) would not be subject to penalties or disincentives

- Three specific conditions:
  - Transparency Conditions
  - Permitted Fees Conditions
  - Openness and Pro-Competitive Conditions
- Maintenance of Certification Requirements

- New 2015 Edition "Cures Criterion"
  - Secure, standards-based API (170.315(g)(10)) – "read-only" focus
  - HL7® FHIR® as base standard
  - SMART App Launch Framework + OAuth 2 + OpenID Connect 1.0
  - Support for provider and patient-access use cases

API Conditions of Certification

Who?

API Technology Supplier: Health IT developer of certified API technology

API Data Provider: Health care organization that deploys the API technology

***API User:* Persons and entities that use or create software applications that interact with API technology**

What?

Applies to all API-focused certification criteria (170.315(g)(7) through proposed (g)(10) and (11))

Practically speaking "FHIR Servers"

How?

The API Condition of Certification applies only to health IT developers and health IT that is certified to the any of the API-focused certification criteria

New API Certification Criteria 170.315(g)(10) to replace (g)(8) Standards-based API for patient and population services

Required Capability(ies)	Applicable Standard(s)	Additional Context
App Registration	None; Dynamic Registration permitted	Associated API CoC
Secure Connection	SMART Application Launch Framework IG	• Must support patient- and clinical- access • Must support access to a single patient's data & multiple patients data • Must support "Standalone Launch" and "EHR Launch" • Refresh tokens with a lifetime of at least 3 months
1st time Authentication & App Authorization + (get refresh token)	OpenID Connect + SMART Application Launch Framework IG	
Data Response (query)	FHIR (Release 2) + ARCH + Argonaut Data Query IG Profiles	
Search	Argonaut Data Query IG Server	
Subsequent Authentication & App Authorization + (new refresh token)	SMART Application Launch Framework IG	
Documentation	None; Must be made publicly accessible	Associated API CoC

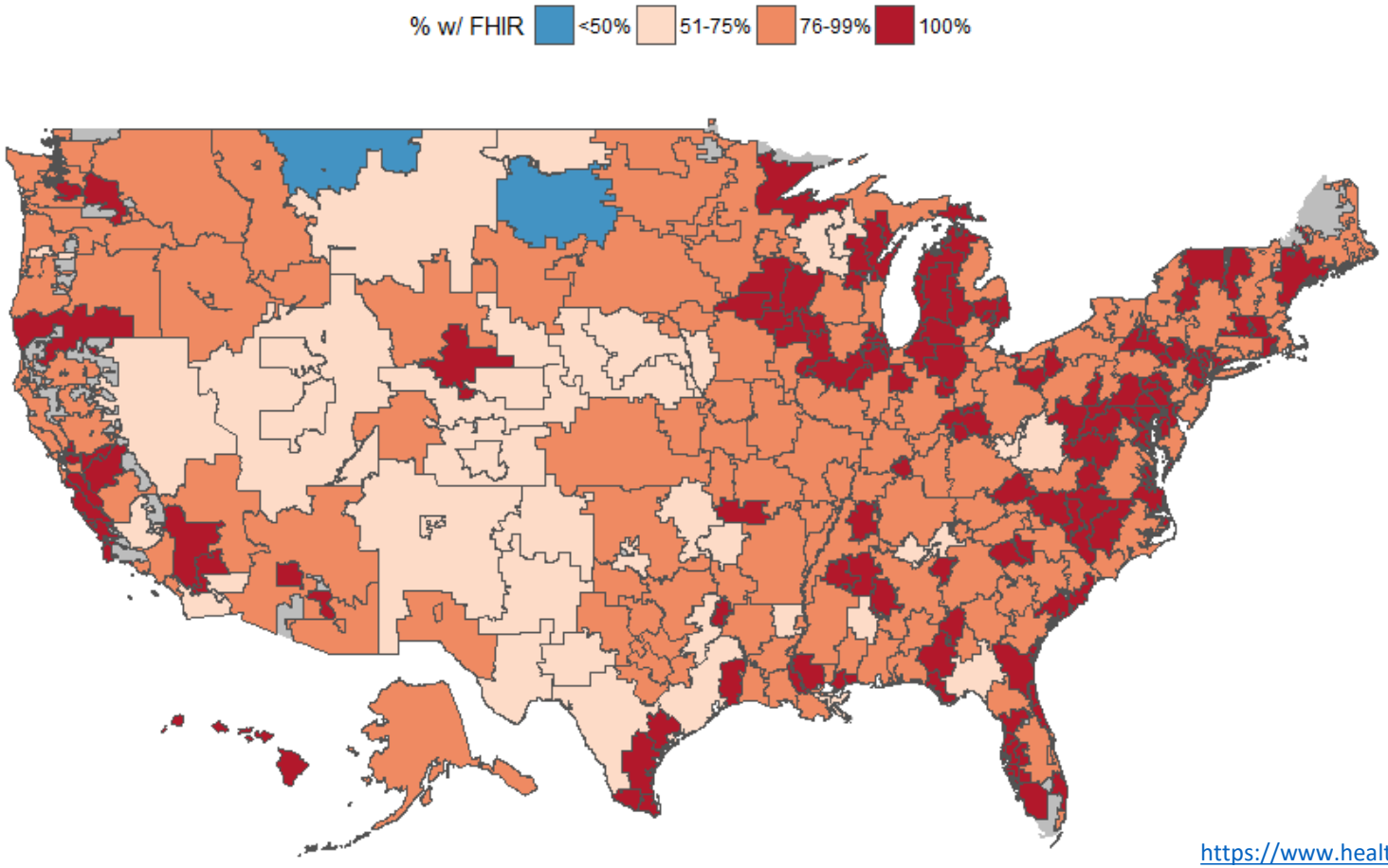
FHIR Server Testing

https://inferno.healthit.gov/inferno/

FHIR Implementation Nationwide

Percent of hospitals with a 2015 Edition certified-API enabled with FHIR

By Hospital Referral Region



Source: CHPL; Medicare EHR Incentive Program
Notes: (1) gray areas = HRR with no hospital; (2) The most recent attestations to the Medicare EHR Incentive Program were used to determine EHR installations for all hospitals. These attestations may not reflect the most currently installed technology for all hospitals. In some cases, %'s may be underestimated for HRRs.

Of the hospitals and Merit-based Incentive Payment System (MIPS) eligible clinicians that use certified products, we found that almost:

- 87% of hospitals
- 69% of MIPS eligible clinicians

are served by health IT developers with product(s) certified to any FHIR version.

https://www.healthit.gov/buzz-blog/interoperability/heat-wave-the-u-s-is-poised-to-catch-fhir-in-2019

The US Core Data For Interoperability (USCDI v1)

Assessment and Plan of Treatment

Care Team Members

Clinical Notes

- Consultation Note
- Discharge Summary Note
- History & Physical
- Imaging Narrative
- Laboratory Report Narrative
- Pathology Report Narrative
- Procedure Note
- Progress Note

Goals

- Patient Goals

Health Concerns

Immunizations

Medications

- Medications
- Medication Allergies

Patient Demographics

- First Name
- Last Name
- Previous Name
- Middle Name (incl. middle initial)
- Suffix
- Birth Sex
- Date of Birth
- Race
- Ethnicity
- Preferred Language
- Address
- Phone Number

Problems

Procedures

Provenance

- Author
- Author Time Stamp
- Author Organization

Smoking Status

Unique Device Identifier(s) for a Patient's Implantable Device(s)

Laboratory

- Tests
- Values/Results

Vital Signs

- Diastolic BP
- Systolic BP
- Body height
- Body weight
- Heart Rate
- Body temperature
- Pulse oximetry
- Inhaled oxygen concentration
- BMI percentile per age and sex for youth 2-20
- Weights for age per length and sex
- Occipital-frontal circumference for children >3 years old

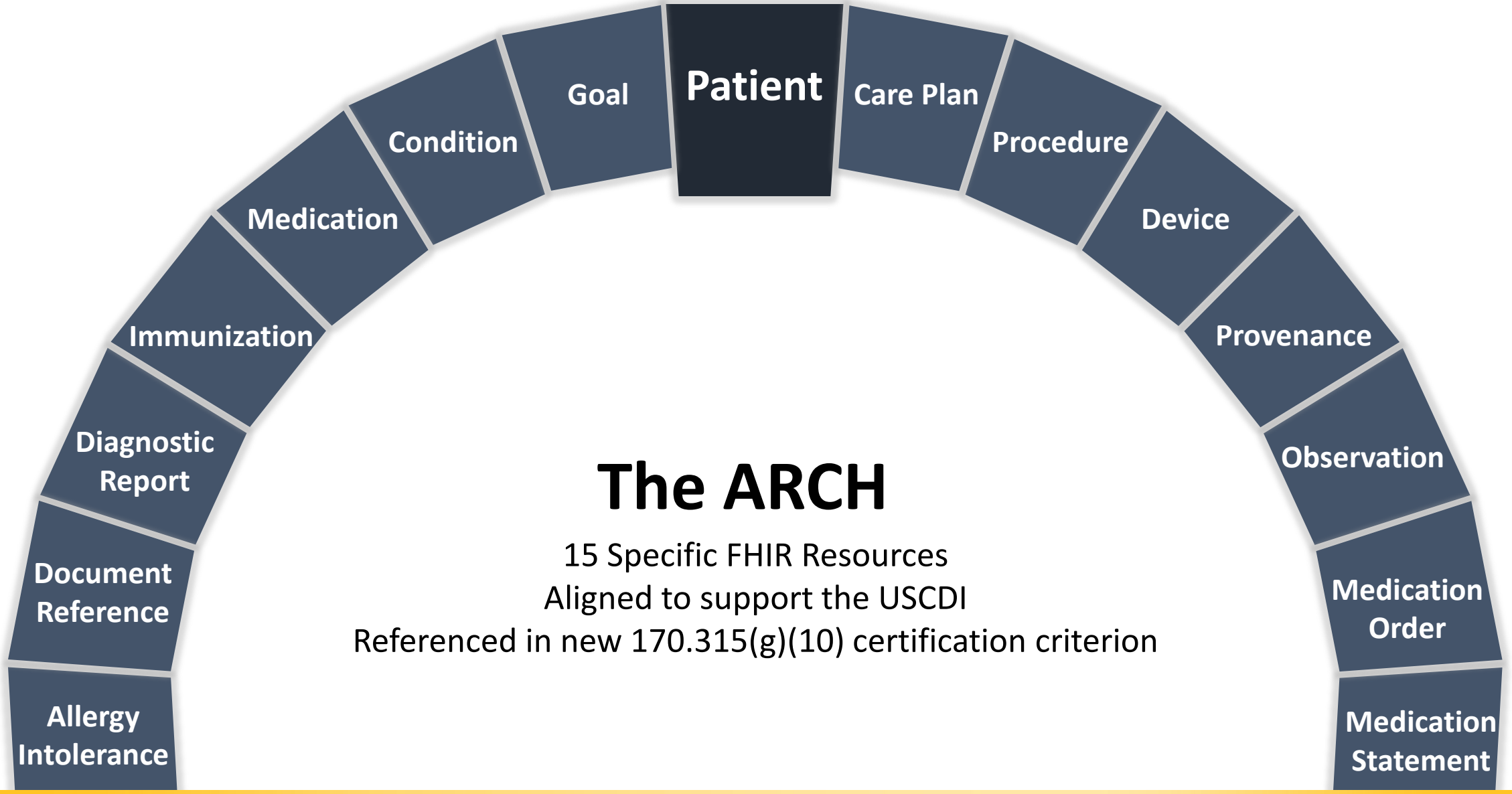
Translating the USCDI into Computable Content

Applicable FHIR Resources were selected to support USCDI Data Classes and Data Elements

USCDI

ARCH

What is the API Resource Collection in Health (ARCH)?



The ARCH

15 Specific FHIR Resources
Aligned to support the USCDI
Referenced in new 170.315(g)(10) certification criterion

API Conditions and Maintenance of Certification High-level Overview

Cures Act Condition

An API Technology Supplier must publish APIs and must allow health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws

Transparency

- Publicly accessible documentation
  - Terms and conditions
  - Fees and structure
  - App developer verification process

Permitted Fees

- Only specific types of fees are permitted
- Must have objective and verifiable criteria
- Three categories of permitted fees
- Must keep detailed records for fees

Openness and Pro-competitive

- Must grant API Data Providers sole authority
- Terms must be non-discriminatory
- All necessary "rights" must be provided
- Must maintain service and support levels

Maintenance of Certification

- An API Technology Supplier must register and enable apps for production use within one business day of completing its verification of an app developer's authenticity
- An API Technology Supplier must support the publication of Service Base URLs (i.e., FHIR API endpoints) for all of its customers and make such information publicly available (in a computable format) at no charge
- An API Technology Supplier with API technology previously certified to § 170.315(g)(8) must provide all API Data Providers with a (g)(10)-certified API within 24 months of a final rule's effective date

The API Conditions of Certification Transparency Conditions

The business and technical documentation published by an API Technology Supplier must be complete. All documentation must be published via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

Material Information

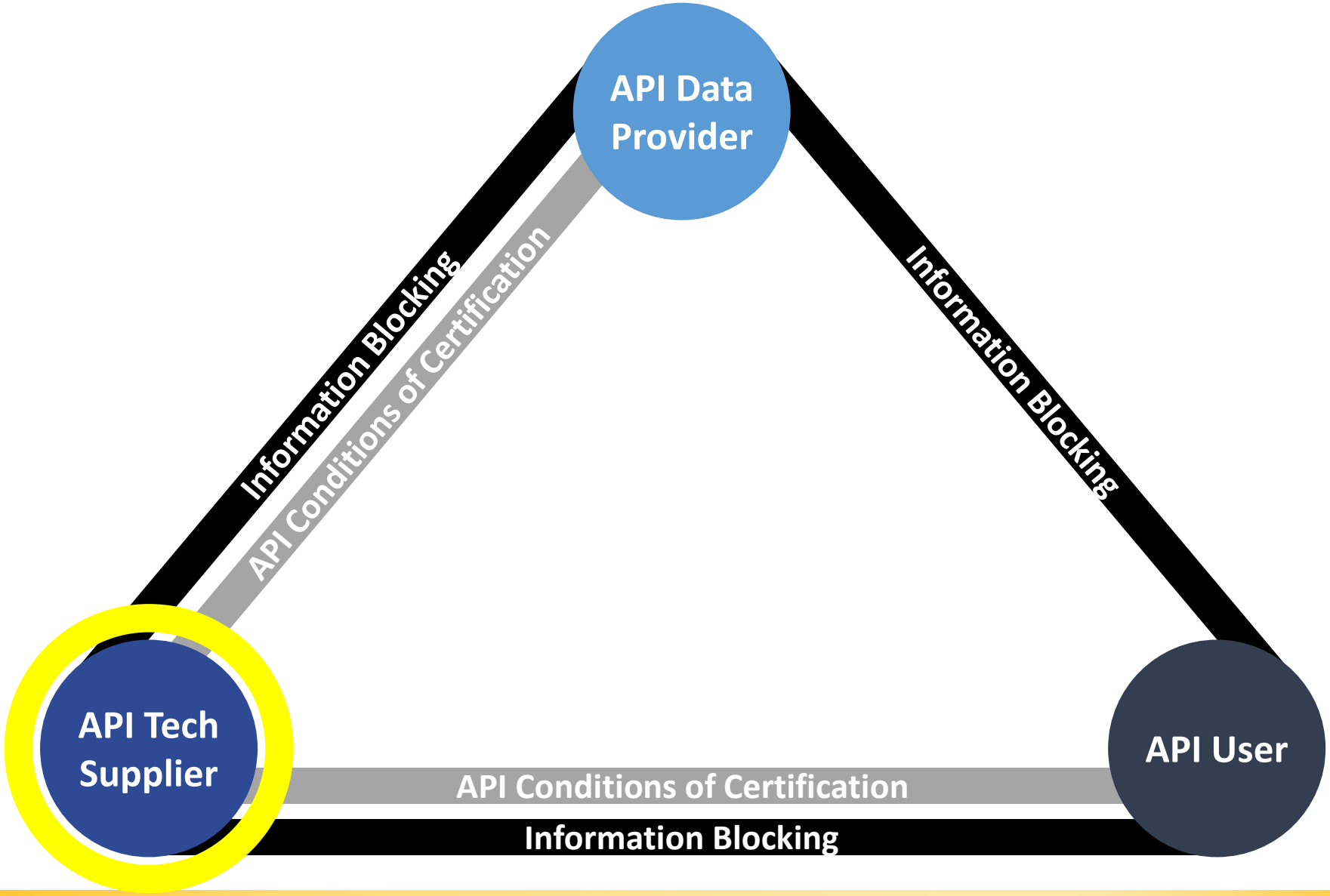
The API Technology Supplier must publish all terms and conditions for its API technology, including any fees, restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be needed to:

(1) Develop software applications to interact with the API technology;
(2) Distribute, deploy, and enable the use of software applications in production environments that use the API technology;
(3) Use software applications, including to access, exchange, and use electronic health information by means of the API technology;
(4) Use any electronic health information obtained by means of the API technology; and
(5) Register software applications.

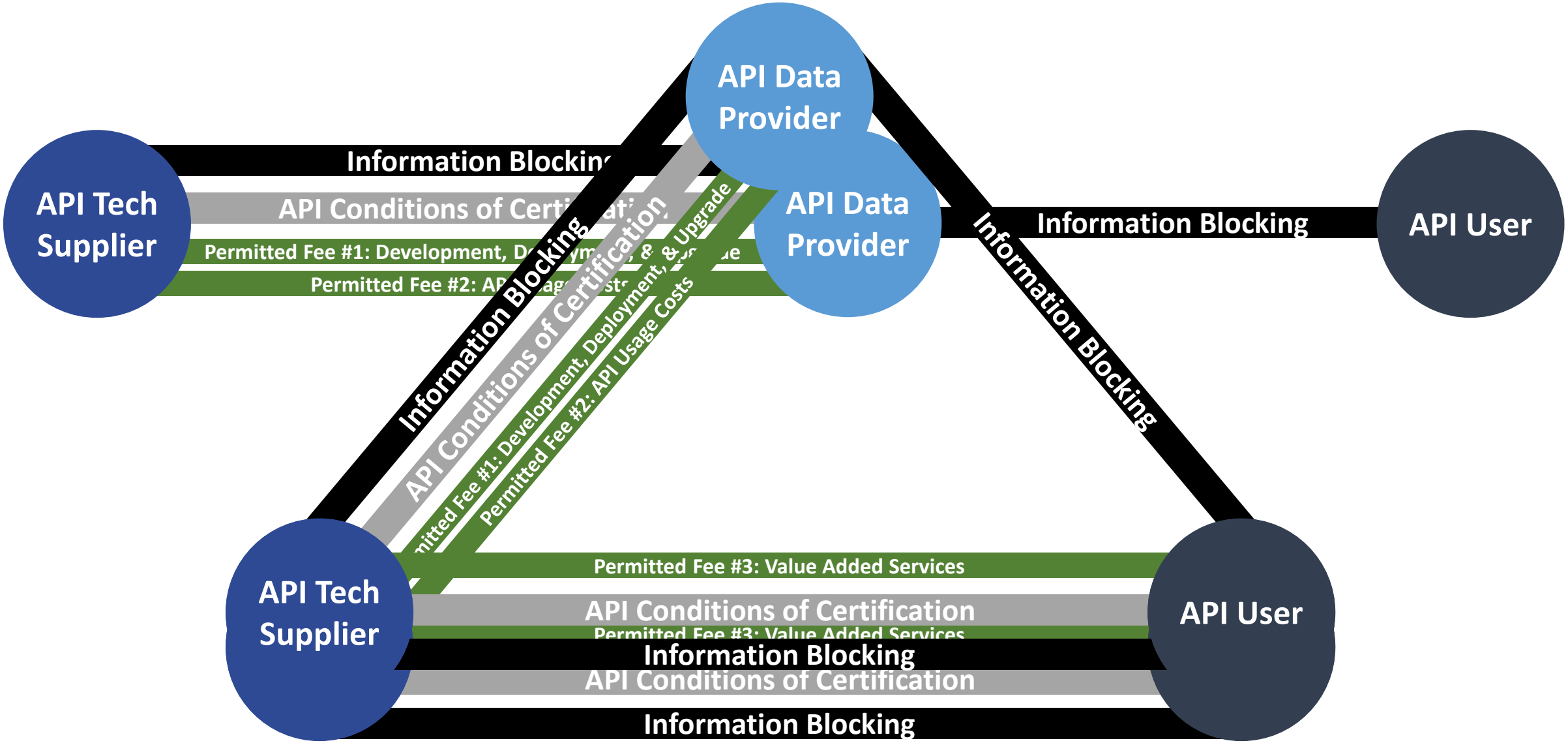
Any and all fees charged by an API Technology Supplier for the use of its API technology must be described in detailed, plain language. The description of the fees must include all material information, including but not limited to:
(1) The persons or classes of persons to whom the fee applies;
(2) The circumstances in which the fee applies; and
(3) The amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee.

An API Technology Supplier is permitted to institute a process to verify the authenticity of application developers so long as such process is objective and the same for all application developers and completed within 5 business days of receipt of an application developer's request to register their software application for use with the API Technology Supplier's API technology.

The API Conditions of Certification & Information Blocking Permitted Fees

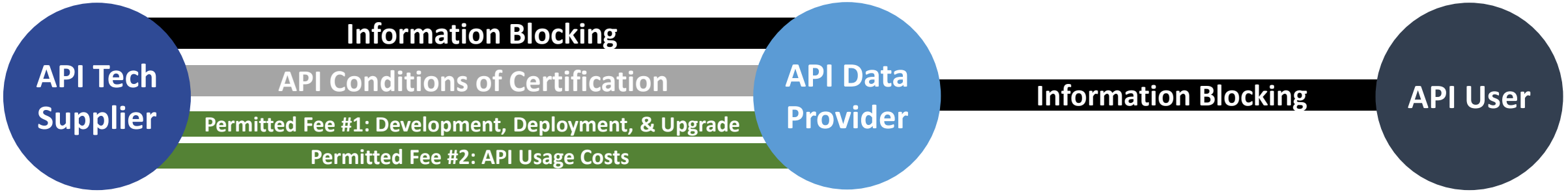


The API Conditions of Certification & Information Blocking Permitted Fees

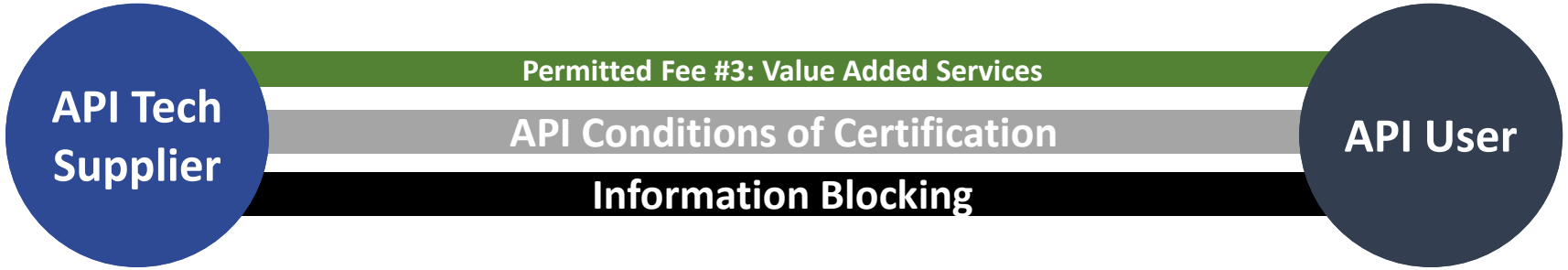


The API Conditions of Certification & Information Blocking Permitted Fees

Scenario 1



Scenario 2



The API Conditions of Certification
Permitted Fees: General Conditions

All fees related to API technology not otherwise permitted are prohibited from being imposed by an API Technology Supplier.

For all permitted fees, an API Technology Supplier must:

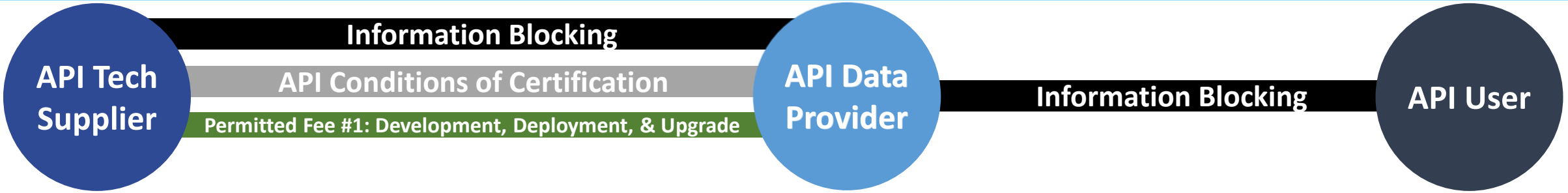
Ensure that fees are based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

Ensure that fees imposed on API Data Providers are reasonably related to the API Technology Supplier's costs of supplying and, if applicable, supporting API technology to, or at the request of, the API Data Provider to whom the fee is charged.

Ensure that the costs of supplying and, if applicable, supporting the API technology upon which the fee is based are reasonably allocated among all customers to whom the API technology is supplied, or for whom the API technology is supported.

Ensure that fees are not based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the API technology in a way that facilitates competition with the API Technology Supplier.

Scenario #1, Permitted Fee #1
Development, Deployment, and Upgrade Fees



- **An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the costs reasonably incurred by the API Technology Supplier to develop, deploy, and upgrade API technology for the API Data Provider.**

- **An API Technology Supplier is NOT permitted to establish "relationship" fees between itself and an API User just because of the API User's connectivity to or mutual business relationship with the API Technology Supplier's customer (i.e., the API Data Provider).**

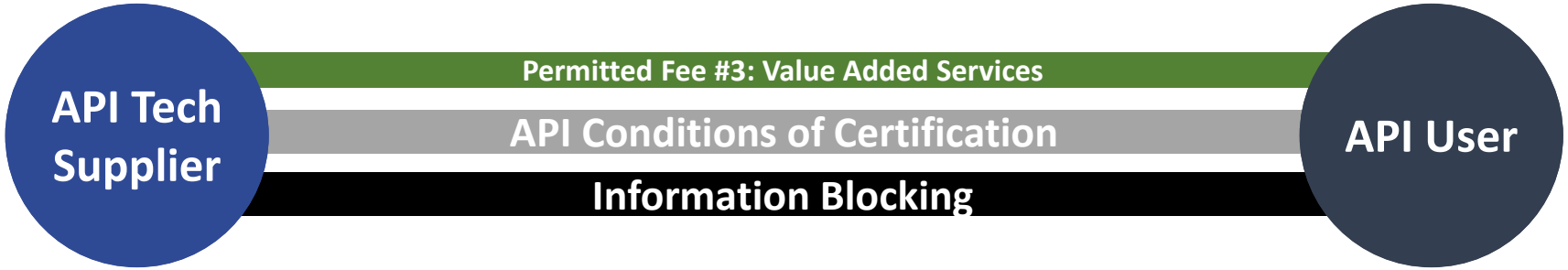
Scenario #1, Permitted Fee #2
API Usage Costs

- **An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the incremental costs reasonably incurred by the API Technology Supplier to support the use of API technology deployed by or on behalf of the API Data Provider.**
- **<u>An API Technology Supplier is only permitted to charge the API Data Provider.</u> If an API User exceeds service established levels, the API Data Provider would be responsible for paying the extra charges.**
- **If an API Data Provider administers the API on its own (i.e., assumes full responsibility), then API Technology Supplier would not be permitted to charge usage fees.**
- **The costs recovered under "usage-based" fees would only be able to reflect "post-deployment" costs.**
- **No particular fee amount, threshold, or methodology is proposed. It is up to the API Technology Supplier to determine consistent with the "general conditions" and information blocking.**

Scenario #1, Permitted Fee #2
API Usage Costs

- **This permitted fee DOES NOT include:**
  - **Any costs incurred by the API Technology Supplier to support uses of the API technology that facilitate a patient's ability to access, exchange, or use their electronic health information.**
  - **Costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets.**
  - **Opportunity costs, except for the reasonable forward-looking cost of capital.**
- **(reiterated) An API Technology Supplier is NOT permitted to establish "relationship" fees between itself and an API User just because of the API User's connectivity to or mutual business relationship with the API Technology Supplier's customer (i.e., the API Data Provider).**

Scenario #2, Permitted Fee #3
Value Added Services Fees



- **An API Technology Supplier is permitted to charge fees to an API User for value-added services supplied in connection with software that can interact with the API technology, provided that such services are not necessary to efficiently and effectively develop and deploy such software (i.e., production-ready software).**
- **Permits API Technology Suppliers to offer market differentiating services that could make it attractive for API Users to develop software applications that can interact with the API technology.**
- **Examples: advanced training, premium development tools and distribution channels, enhanced compatibility/integration testing assessments, co-branded integration, co-marketing arrangements, promoted placement in "app store."**
- **API Technology Suppliers would be able to administer their own "app stores" provided that they do not violate this condition of certification and information blocking policies.**
  - ***for example, if a software developer's app were required to go through a paid listing process as a precondition to be able to be deployed (and generally accessible) to the API Technology Supplier's health care provider customers to use, this would not be a permitted fee under this Condition of Certification, would constitute special effort, and could raise information blocking concerns.***

The API Conditions of Certification
Openness and Pro-Competitive Conditions (1)

An API Technology Supplier must grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider.

Non-Discriminatory Terms

An API Technology Suppler must provide API technology to API Data Providers on terms that are no less favorable than it provides to itself and its own customers, suppliers, partners, and other persons with whom it has a business relationship.

The terms on which an API Technology Supplier provides API technology must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

An API Technology Supplier must not offer different terms or service on the basis of:

1) **Whether the API User with whom an API Data Provider has a relationship is a competitor, potential competitor, or will be using electronic health information obtained via the API technology in a way that facilitates competition with the API Technology Supplier.**

2) **The revenue or other value the API User with whom an API Data Provider has a relationship may derive from access, exchange, or use of electronic health information obtained by means of API technology.**

The API Conditions of Certification Openness and Pro-Competitive Conditions (2)

An API Technology Supplier must grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider.

Rights to access and use API technology

An API Technology Supplier must have and, upon request, must grant to API Data Providers and their API Users all rights that may be reasonably necessary to access and use API technology in a production environment, including:

1) **For the purposes of developing products or services that are designed to be interoperable with the API Technology Supplier's health information technology or with health information technology under the API Technology Supplier's control;**

2) **Any marketing, offering, and distribution of interoperable products and services to potential customers and users that would be needed for the API technology to be used in a production environment; and**

3) **Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.**

An API Technology Supplier must not condition any of the rights described on the requirement that the recipient of the rights do, or agree to do, any of the following:

1) **Pay a fee to license such rights, including but not limited to a license fee, royalty, or revenue-sharing arrangement.**
2) **Not compete with the API Technology Supplier in any product, service, or market.**
3) **Deal exclusively with the API Technology Supplier in any product, service, or market.**
4) **Obtain additional licenses, products, or services that are not related to or can be unbundled from the API technology.**
5) **License, grant, assign, or transfer any intellectual property to the API Technology Supplier.**
6) **Meet additional developer or product certification requirements.**
7) **Provide the API Technology Supplier or its technology with reciprocal access to application data.**

The API Conditions of Certification
Openness and Pro-Competitive Conditions (3)

An API Technology Supplier must grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider.

Service and Support Obligations

An API Technology Supplier must provide all support and other services reasonably necessary to enable the effective development, deployment, and use of API technology by API Data Providers and their API Users in production environments.

An API Technology Supplier must make reasonable efforts to maintain the compatibility of its API technology and to otherwise avoid disrupting the use of API technology in production environments.

Except as exigent circumstances require, prior to making changes or updates to its API technology or to the terms and conditions thereof, an API Technology Supplier must provide notice and a reasonable opportunity for its API Data Provider customers and registered application developers to update their applications to preserve compatibility with API technology and to comply with applicable terms and conditions.

Don’t Miss
Requests for Comment

- **Four options proposed for FHIR Standard(s) adoption**
  - **Option 1: Just FHIR Release 2 (proposed)**
  - **Option 2: FHIR Release 2 and Release 3 (as either one for certification option)**
  - **Option 3: FHIR Release 2 and Release 4 (as either one for certification option)**
  - **Option 4: Just FHIR Release 4**

- **For the DocumentReference and Provenance resources, which are currently present in the base FHIR standard, we request comments on the minimum “search” parameters that would need to be supported**

- **On any additional specific “permitted fees” not addressed above that API Technology Suppliers should be able to recover in order to assure a reasonable return on investment. Furthermore, we request comment on whether it would be prudent to adopt specific, or more granular, cost methodologies for the calculation of the permitted fees.**

- **On a reasonable upper bound for Refresh Token period of use**

- **On whether we should require support for OAuth 2.0 Dynamic Client Registration Protocol**