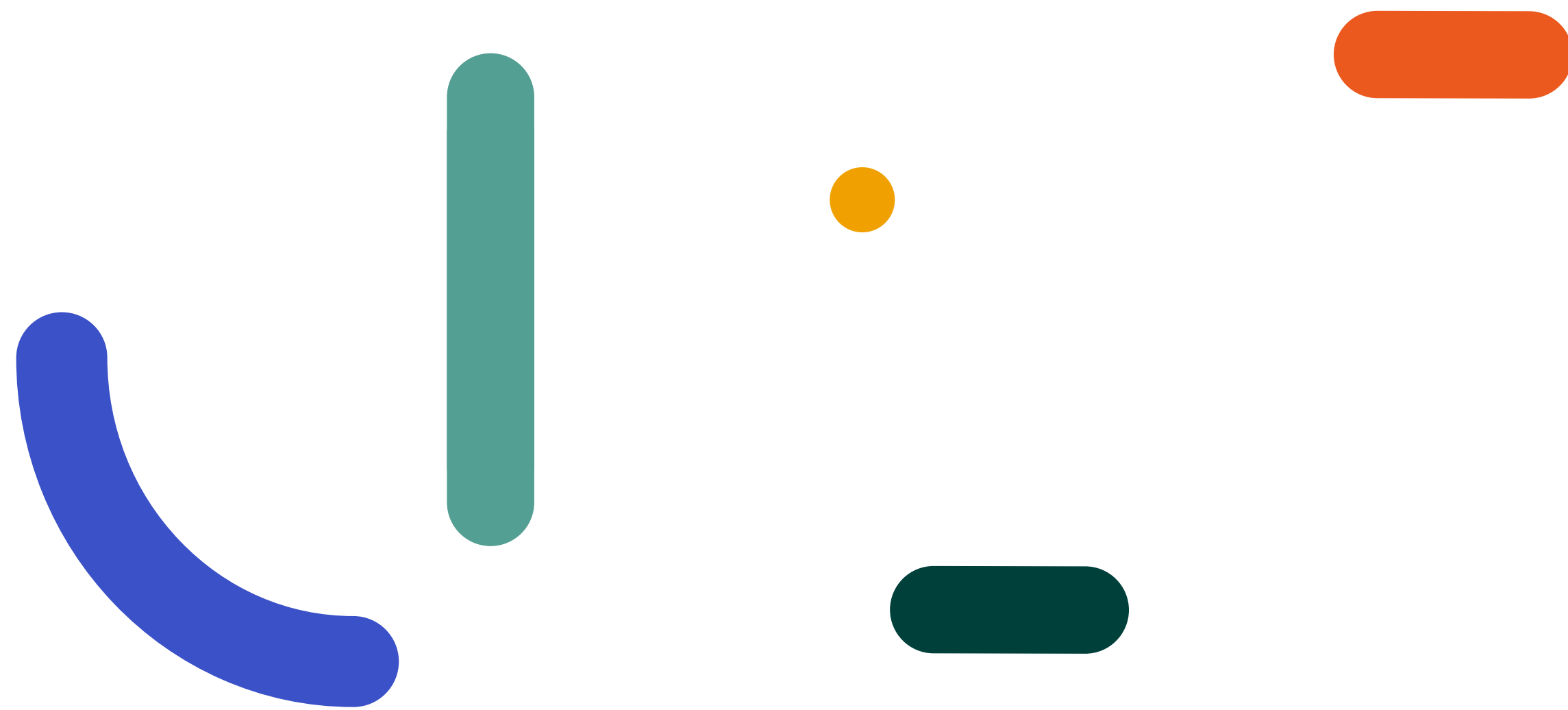# Treatment
Purpose of Use Overview

→ Overview

**Can your organization access an extraordinary amount of
patient data through Particle's API?
It depends what your Purpose of Use is.**

Under HIPAA, a covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for Treatment, Payment, or Operations (TPO) uses. From HHS: "Ready access to treatment and efficient payment for health care, both of which require use and disclosure of protected health information, are essential to the effective operation of the health care system. In addition, certain [administrative] health care operations … are essential to support treatment and payment." So basically, because these are essential activities, entities requesting don't need consent from the patient whose records they are requesting at the federal level.

→ Treatment, Payment, and Operations (TPO)

Treatment (Particle's #1 Primary Use)

"Treatment" generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another. Basically: providers are directly involved in the treatment or management of care of their patients.

Examples include:

↘

A patient schedules an appointment with a primary care physician at a clinic. At the time of scheduling the appointment, the clinic automatically queries Particle's API and instantaneously uploads that patient's medical records into their patient chart. This helps the physician have a clear and holistic picture of the patient even before seeing them, as well as expediting the onboarding process.

↘

An individual signs up for a chronic care online program to help them better manage their condition. Once the individual registers, this triggers the digital health company to query Particle's API to retrieve medical records on the patient and upload them into the patient chart. This information is used by case managers and physicians to better treat and personalize care for the individual.

↘

A patient goes to a gastroenterologist and is only interested in what past procedures and diagnoses the patient had. The gastroenterologist tells its staff that once a patient schedules a consultation type of appointment, to only receive past procedures and diagnoses. So whenever there is a new consultation, the practice queries Particle's FHIR API to only receive procedure and diagnosis resources and upload that information into a patient's chart.
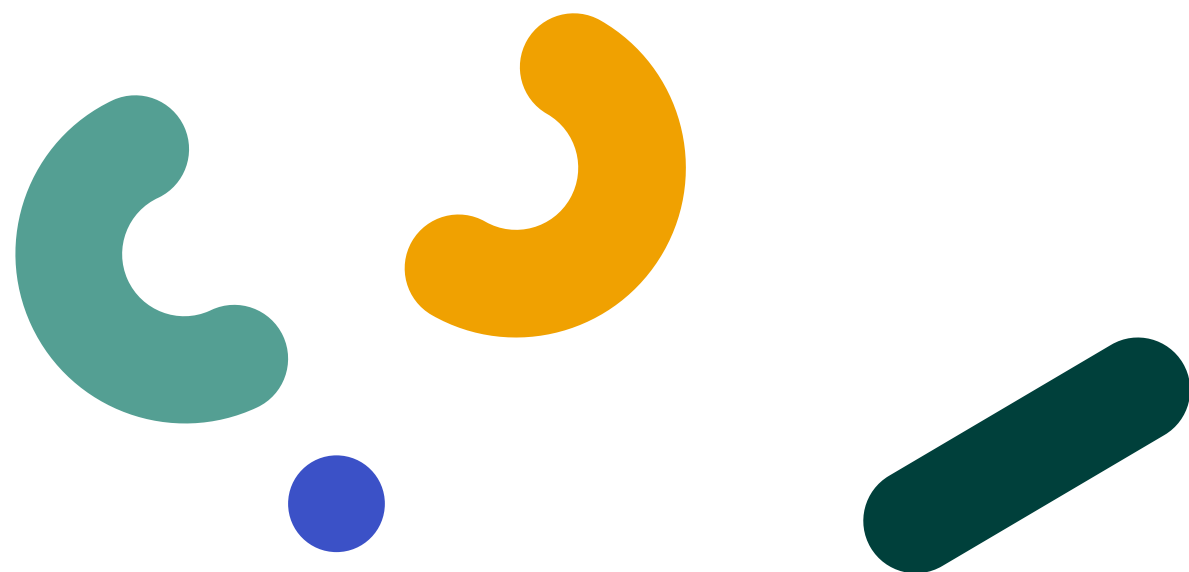
Operations

"Health care operations" are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. Basically: The things within a healthcare organization that no one wants to do, but needs to be done to ensure that the other functions of the organization (treatment and payment) are working seamlessly (think of policy creation, audits, requesting data, etc.)

Operations activities may include:

↘

Claims Adjudication: the process of paying claims submitted or denying them after comparing claims to the benefit or coverage requirements

- You see a doctor. A medical claim is submitted for the services the doctor conducted during the visit. The insurance company determines your financial responsibility to the provider. This process is referred to as claims adjudication. The insurance company can decide to pay the claim in full, deny the claim, or to reduce the amount paid to the provider.

- Now you may ask how this relates to Particle and what type of data we can provide to help out with this. Using Particle, insurance companies can instantly request and retrieve Proof-of-Loss statements (a document that states the amount of money the policyholder is requesting from the insurance carrier) and confirm clinical data to process a claim.
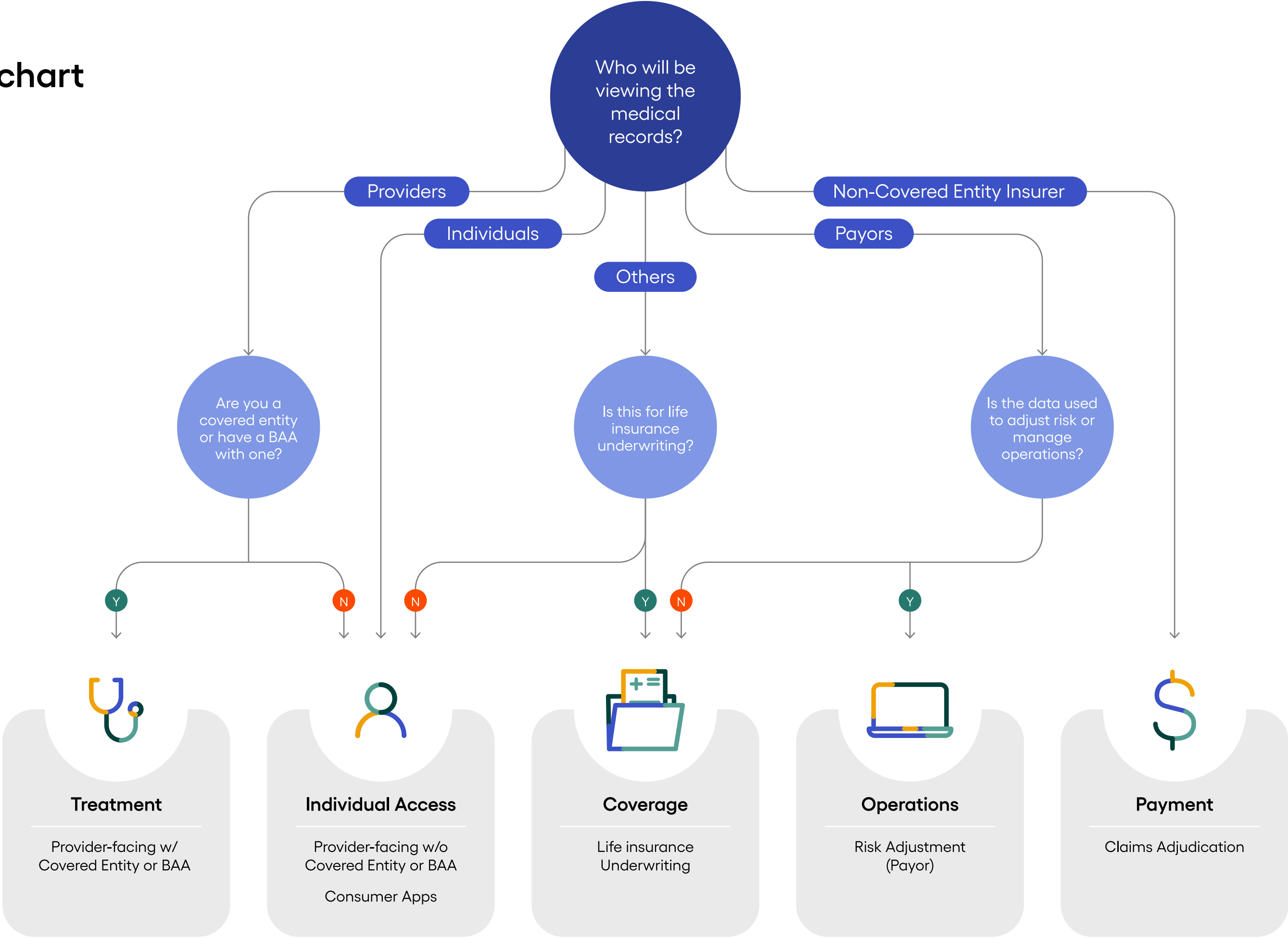
↘

Risk Adjustment: the method to offset the cost of providing health insurance for individuals—such as those with chronic health conditions—who represent a relatively high risk to insurers

- This means that organizations can run lists for large numbers of policyholders for Risk Adjustment and review, and then batch submit large data requests.

Payment

"Payment" encompasses the various activities of health care providers to obtain payment or be reimbursed for their services; and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. Basically: the activities an organization does to get paid (through direct payments or through reimbursements) and deal with all of the insurance stuff that goes on behind the scenes. Payment activities may include the determining of eligibility or coverage under a plan and adjudicating claims; risk adjustments; billing and collection activities and reviewing health care services for medical necessity, coverage, justification of charges, etc.

Purpose of Use Flowchart

Who will be viewing the medical records?

Providers

Individuals

Others

Payors

Non-Covered Entity Insurer

Are you a covered entity or have a BAA with one?

Is this for life insurance underwriting?

Is the data used to adjust risk or manage operations?

Y

N

N

Y

N

Y

Treatment

Provider-facing w/ Covered Entity or BAA

Individual Access

Provider-facing w/o Covered Entity or BAA

Consumer Apps

Coverage

Life insurance Underwriting

Operations

Risk Adjustment (Payor)

Payment

Claims Adjudication

→ Expansion of POUs

Now that the information blocking provisions of the 21st Century Cures Act Final Rule ("Anti-Information Blocking") rules are in effect, we can expand into other use cases, like Individual Access. Before Anti-Information Blocking, while a patient technically had the right to access and share their own information, provider institutions and their associated systems were not obligated to share that information back to the patient. There were no penalties associated with not sharing, no way to understand the reason for not sharing, and no meaningful oversight to discern who was sharing information– who was not. Under the Anti-Information Blocking provisions, however, all of this changes. Instead of requiring a reason to share the information requested, providers and their systems now need a reason not to share the information requested. This means that you, yourself, your mom, your friend, and your favorite barista have the legal right to access their own medical records– and EMRs are unable to say no or withhold that information (*there are some exceptions.)

Individual Access

Let's say you're a leader at a digital health company that has an app for consumers that stores their medical record information in one place. You find Particle Health through a cool, fun newsletter your friend sent you (hey Up and Atom). You learn that you can use Particle to retrieve individuals' medical records and allow them to store those records in one centralized location– your app. Once a user signs up for your app, they go through the identity verification and authorization process. Once this is complete, this triggers a query to Particle's API to retrieve medical records for that user. Suddenly, you've generated individual access right through the user's phone.
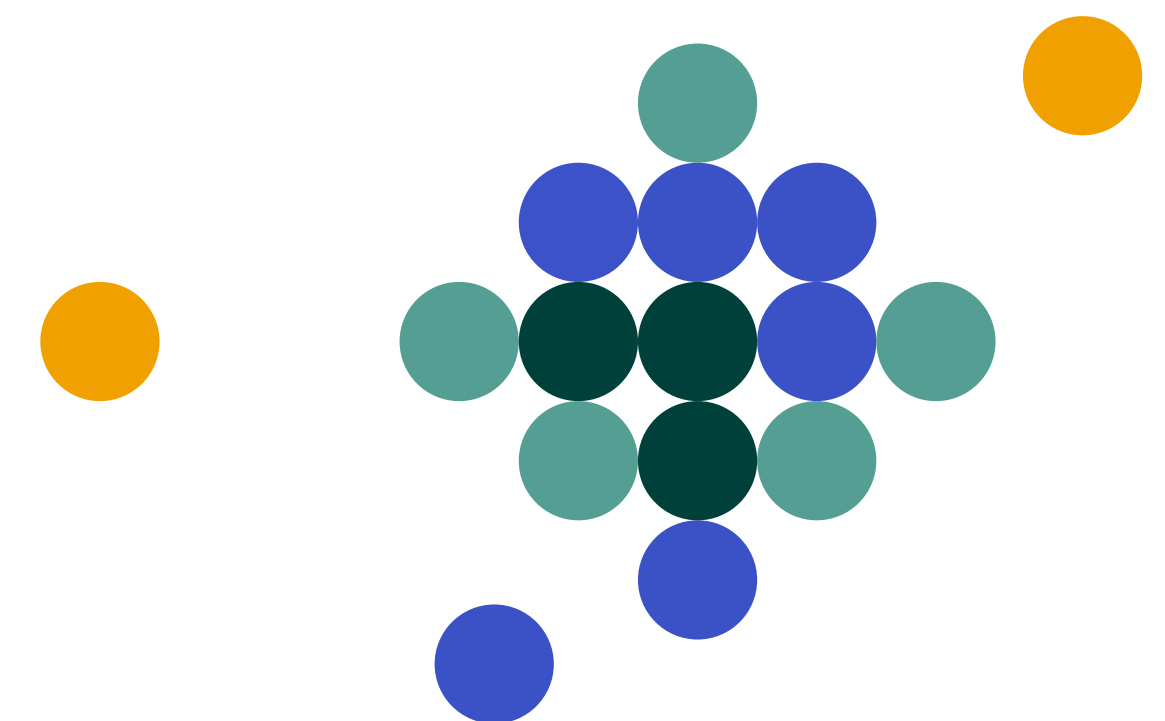
Coverage

Say you want to get life insurance. When you go through this process, the underwriters at the life insurance company may want to review your past medical records to determine risk, and therefore your policy amount. Their usual and traditional method of obtaining your medical records would be through something called an Attending Physician Statement (APS) where they go directly to your provider(s) to get these records.

Let's take a look at the process:

1. You sign a form that the life insurance company provides, essentially giving permission to the insurance company to request medical records from your provider.
2. The insurance company faxes this form over to the medical office.
3. The form is triaged to the staff member who oversees medical records.
4. Staff ensures the signatures are correct and the that you're an active patient (active patient usually means they have seen the provider within 7 years).
5. The staff member counts how many pages are in your medical record.
6. The medical office sends an invoice to the insurance company based on how many pages there are in the record.
7. The insurance company provides a credit card number over the phone or sends a check.

8. The office awaits the payment
9. The office then prints out the pages of the record and prepares it.
10. The office administrator mails the record to the insurance company.
11. The insurance company confirms they received the records.

Imagine this process for every individual applying for life insurance. That's a lot of time, paper, and stamps.

Now let's say the life insurance company is using Particle. Picture this: you go to apply for life insurance. You enter your basic demographic information to apply, as well as any other basic information. The insurance company has a form within the application flow asking if you consent for them to retrieve your medical records. You accept and sign. You go through an identity verification process to make sure you are you. The life insurance company gets your records in a matter of minutes. Underwriters can assess your risk quicker and more efficiently (or they can analyze the data returned to automatically calculate risk and the associated policy).

Particle just took this, what could be, month-long process and boiled it down to a few minutes to get medical records. This is where we see the future of sharing medical records. Efficient, fast, and eliminating the burdens all around.

Your Treatment PoU Qualification Guide:

1. Your workflow
   a. How does data flow through the business?
   b. How does your company handle patient data today (if at all)
   c. How you plan to handle patient data using Particle's API?

2. Who are the end users (title, medical background, responsibilities, etc.) that will be querying for, receiving, and using the data?
   a. Do you have a BAA in place with a covered entity?

3. Does your company / someone in your company have an NPI #? (Are you a covered entity?)

4. Are there any secondary intended uses for the data?

5. Are you absolutely certain you meet HHS's definition to qualify?