



PCM

Patient Consent Manager

סטאטוס והיערכות לתחילת פיתוח

נובמבר 2025

אג'נדה

תכולות המערכת <<

תוכנית עבודה PCM <<

ארכיטקטורה ומשימות הפיתוח של הארגונים - PCM ו NTN <<

המשך הפעילות - Next Steps <<

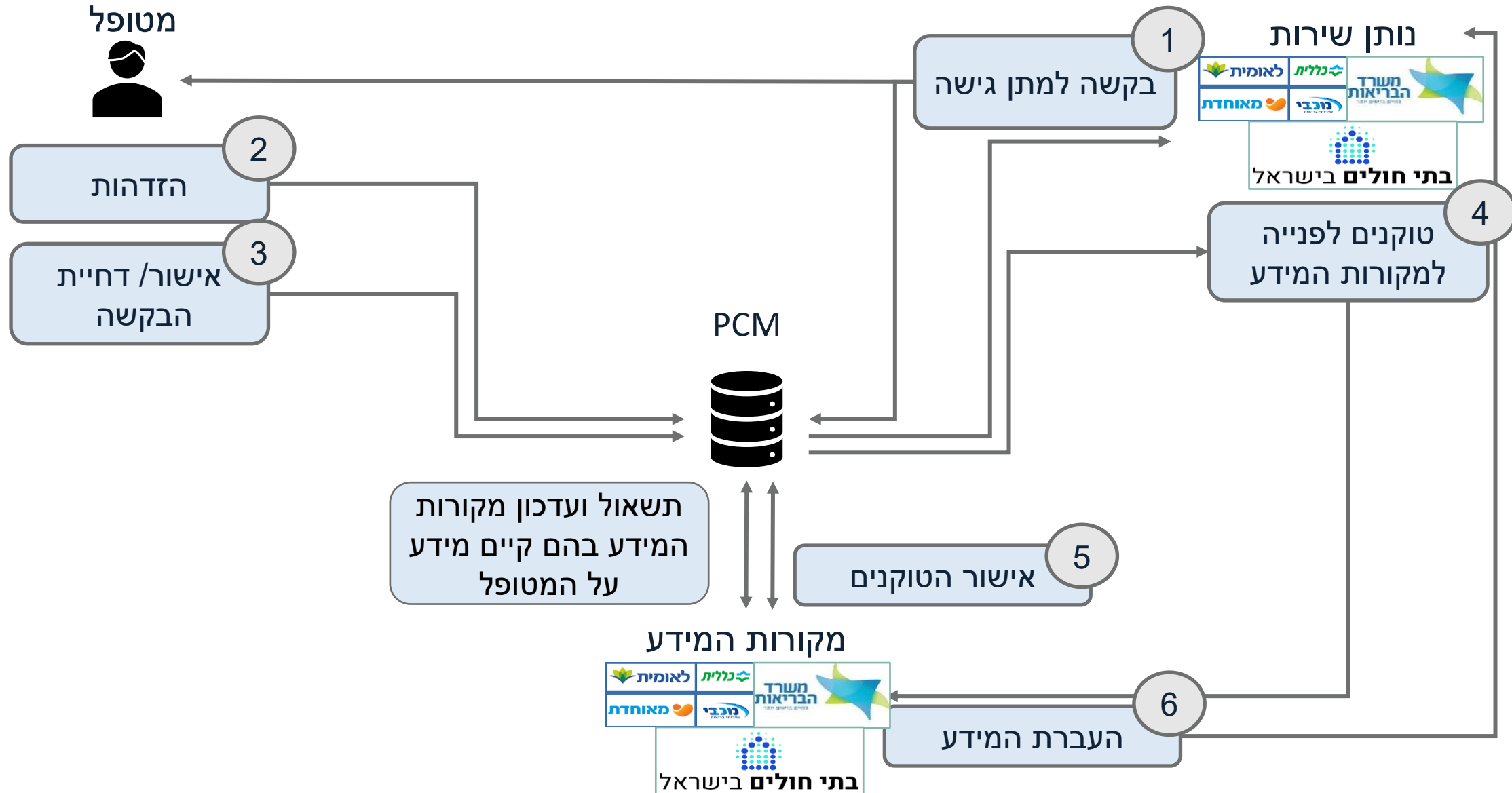
שאלות <<

במסגרת יישום חוק ניווד מידע, משרד הבריאות נדרש להקים

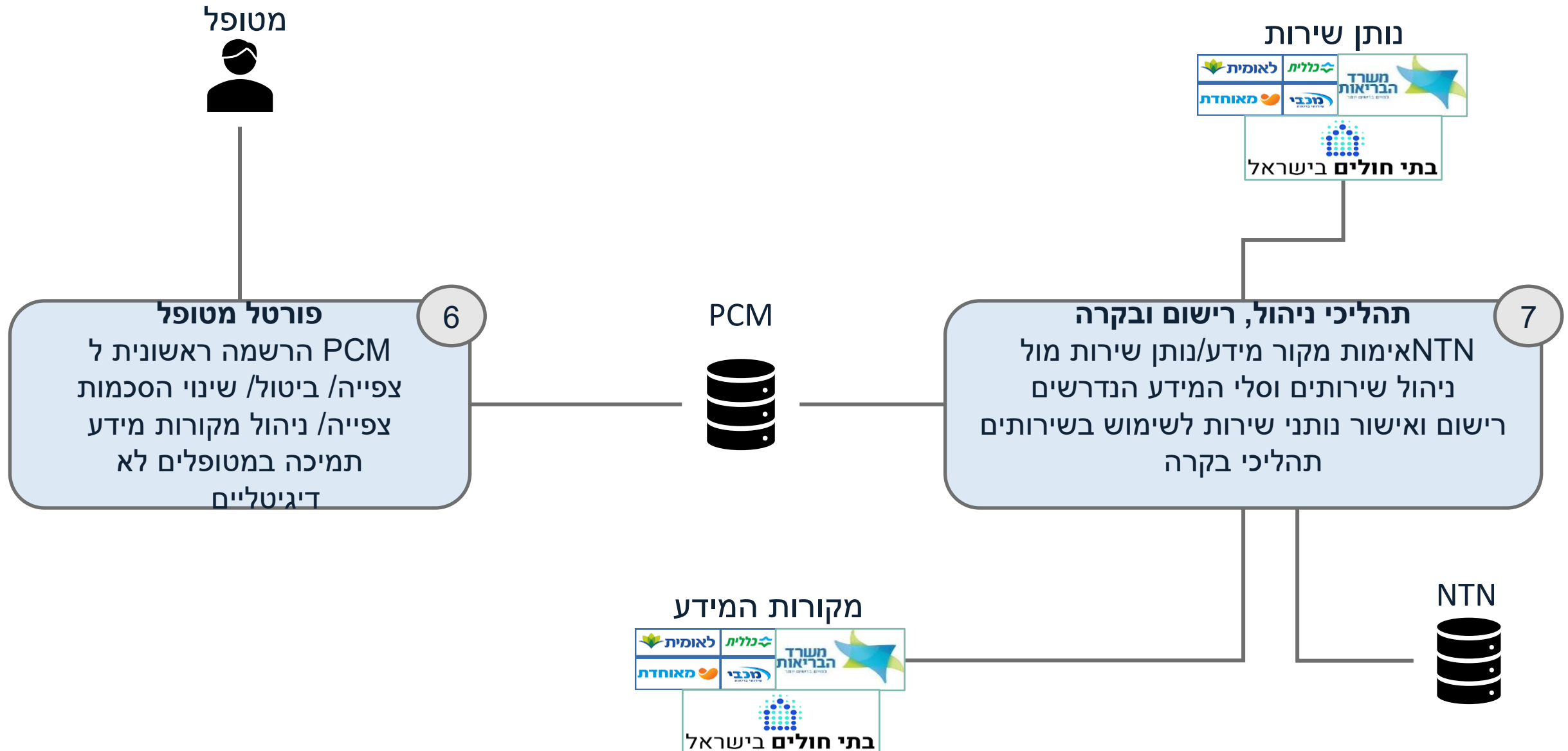
מערכת מרכזית לניהול הסכמות מטופלים,

שתשמש את כלל הארגונים המעבירים ומקבלים את המידע

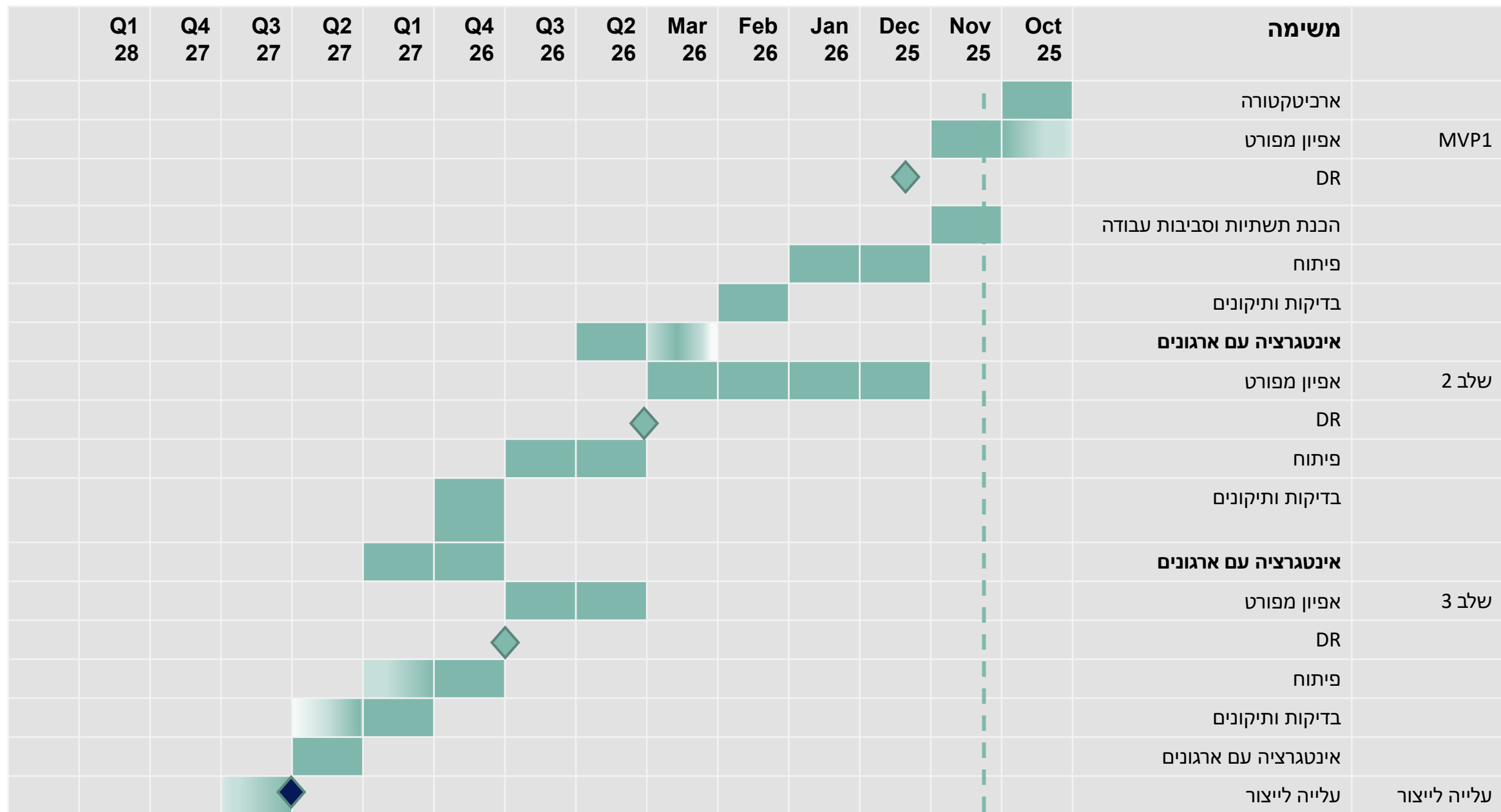
שחקנים ותהליכים מרכזיים



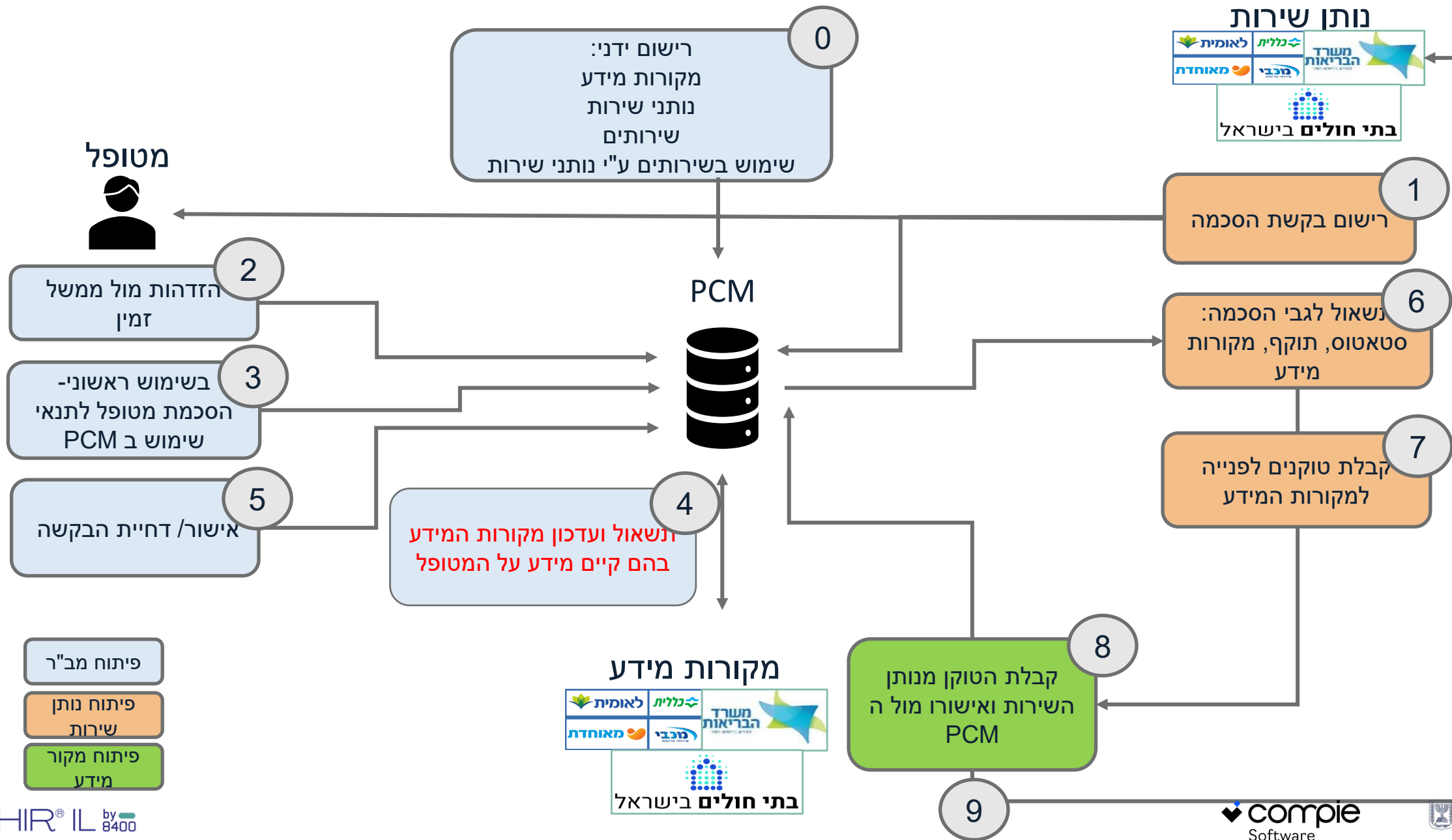
שחקנים ותהליכים מרכזיים



תוכנית עבודה PCM



תכולות MVP1



אינטגרציה החל ממרץ 26

מקור מידע

- קבלת הטוקן מנותן השירות ואישורו מול ה PCM

נותן שירות

- רישום בקשת הסכמה
- תשאול לגבי הסכמה: סטאטוס, תוקף, מקורות מידע
- קבלת טוקנים מה PCM לפנייה למקורות המידע

אינטגרציה החל מדצמבר 26

מקור מידע- כל הארגונים

- רישום מקור מידע ל PCM
- ניהול מקורות מידע עבר מטופל
- אופציונאלי- אישור שירות

מקור מידע- קופות, צה"ל ושב"ס בלבד

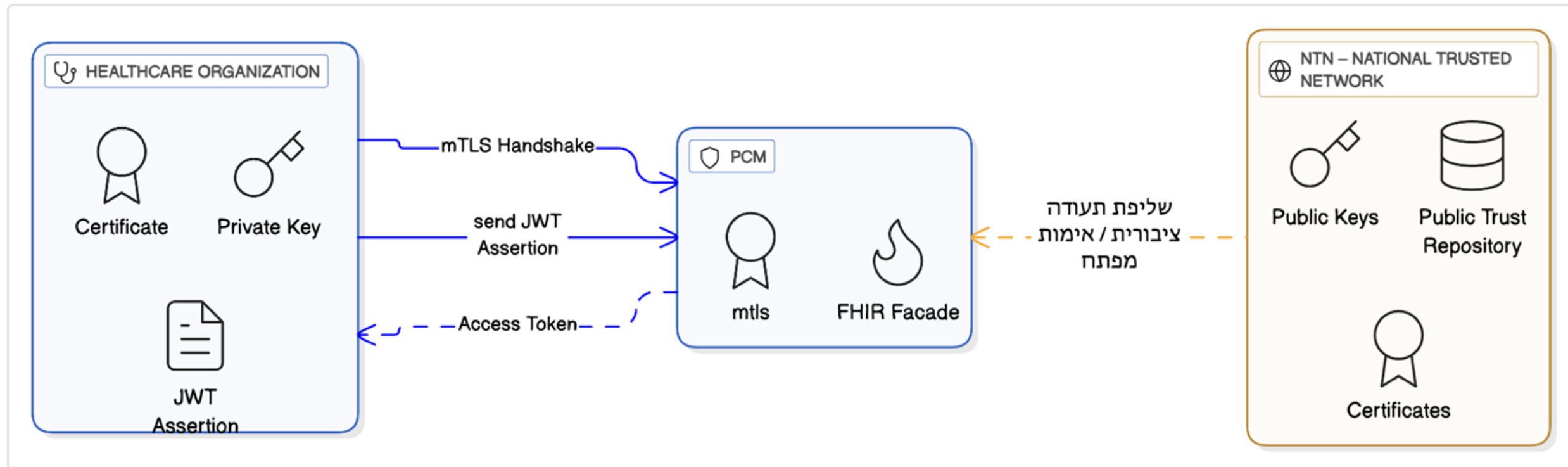
- הזדהות מטופל מול ה PCM- אימות פרטים ושליחת נתוני דמוגרפיה וחוסים
- Re-direct מאתר הקופה ל PCM

אינטגרציה החל מדצמבר 26

נותן שירות

- רישום נותן שירות ל PCM
- רישום וניהול שירות
- רישום שימוש בשירות
- רישום עובדים לטובת סיוע למטופלים לא דיגיטלים
- אופציונאלי- רישום לשירות notifications על אישור/ דחיית הסכמה

ארכיטקטורה



ארכיטקטורה

הארגון מחזיק תעודה דיגיטלית (Certificate) שהונפקה על ידי גוף מאשר (CA) ונרשמה במאגר האמון הלאומי (NTN). התעודה כוללת מפתח ציבורי, והארגון שומר אצלו את המפתח הפרטי התואם.



יצירת – JWT Assertion הארגון יוצר מסמך חתום דיגיטלית (JWT) המהווה הוכחת זהות. החתימה נעשית באמצעות המפתח הפרטי של הארגון.



פתיחת חיבור מאובטח – (mTLS) הארגון ומערכת PCM מקיימים תקשורת הדדית מוצפנת, שבה כל צד מאמת את זהותו באמצעות התעודה הדיגיטלית שלו. ה־JWT נשלח בערוץ ה־mTLS למערכת PCM.



אימות במערכת – PCM המערכת שולפת מה־NTN את המידע הציבורי על הארגון (תעודה / מפתח ציבורי, מאמת את חתימת ה־JWT ומוודאת שהתעודה תקפה ולא בוטלה.



הנפקת Access Token – לאחר אימות מוצלח, המערכת מנפיקה לארגון אסימון גישה קצר טווח, המשמש אותו לקריאות עתידיות לממשקי ה־API של PCM למשל (FHIR תוקף הטוקן 30 שניות).





תשתית NTN National Trusted Network

תפיסת פיתרון וארכיטקטורה
11.11.2025

הגדרות ומטרות תשתית NTN

הגדרה:

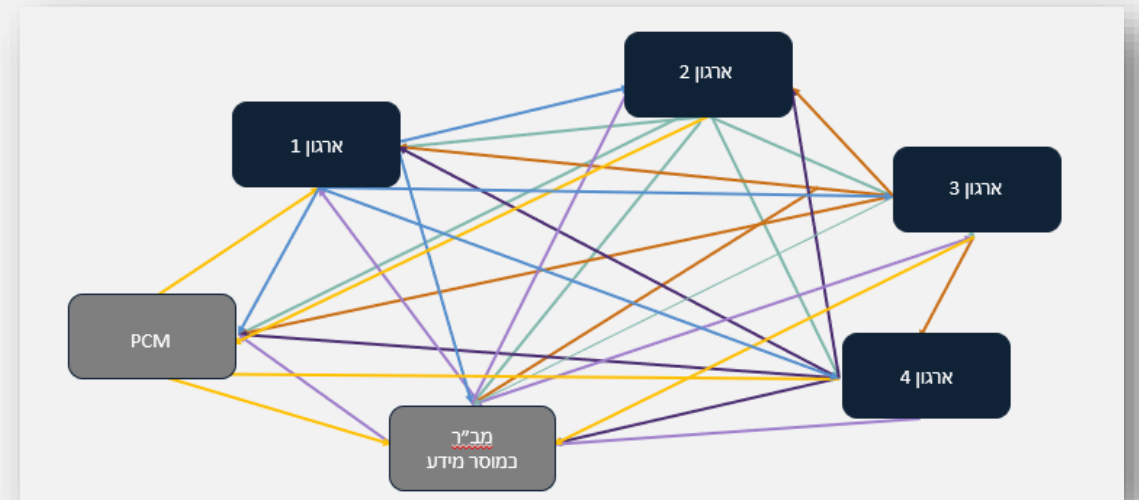
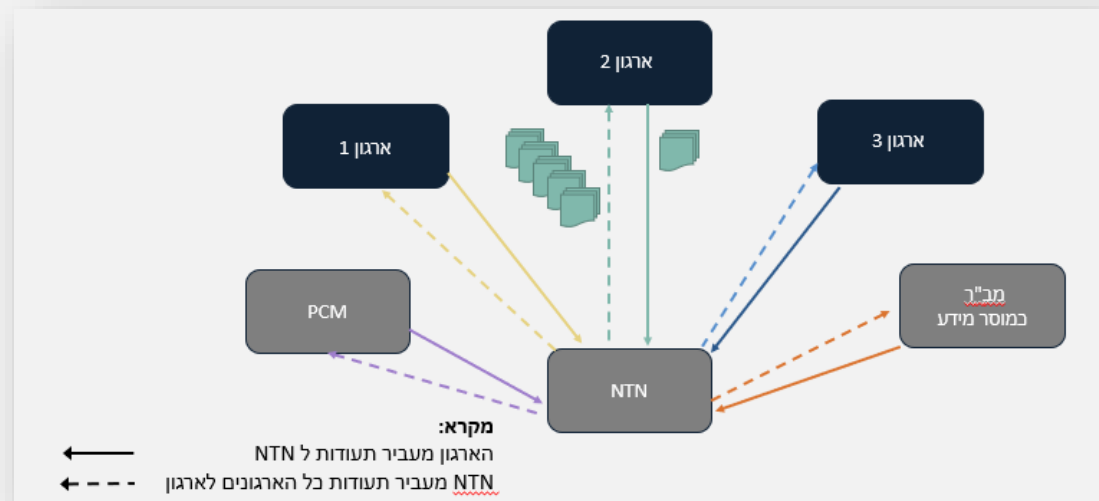
הקמת תשתית לאומית לניהול תעודות קריפטוגרפיות עבור רשת שיתוף הלאומית - (NTN – National Trusted Network)

תרחיש שימוש

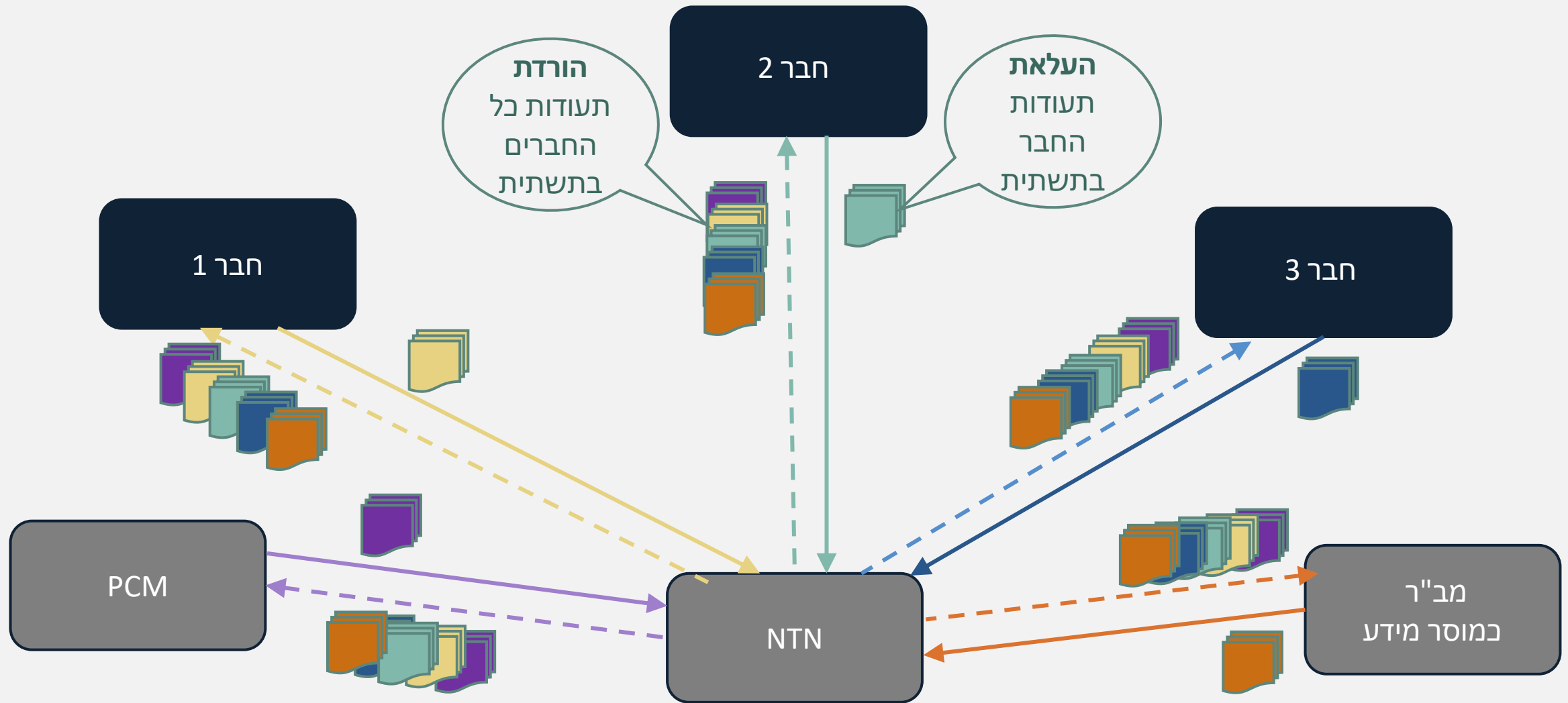
עבור הפרויקטים בהם ארגוני הבריאות מתבקשים לשתף נתונים ביניהם באמצעות שירותי API בצורה מאובטחת, במקום שכל אחד יעביר לכל הארגונים את תעודות הקריפטוגרפיות,

תשתית NTN:

1. תקבל מכל חבר בתשתית את תעודות קריפטוגרפיות של אותו חבר.
2. ותעביר את כל תעודות הקריפטוגרפיות לכל החברים.



העברת תעודות בין ארגונים עם תשתית NTN עבור פרויקט ניוד מידע



עקרונות

- ✓ שימוש בתעודות חתומות בצורה ידנית או קנויות מב"ר לא ינפיק תעודות לחברים בתשתית
- ✓ תשתית NTN לא תפנה לארגונים אלא **הארגונים יפנו לתשתית NTN** באמצעות שירותי API המפורסמים ע"י תשתית NTN.
- ✓ **במקרה חירום** בו נדרש לחסום ארגון מלפנות לשאר הארגונים (לדוגמא : גניבת תעודה / מתקפת סייבר על הארגון), תשתית NTN תסיר את תעודותיו מהתשתית **ותוך זמן קצר , הארגון יהיה חסום** (פניותיו לא יכובדו ע"י ארגונים האחרים).

יישום ראשון: פרויקט ניווד מידע

פיתוח נדרש

- **פיתוח פניה ל API של תשתית NTN** מתוך client (טופס, מערכת, תהליך וכדו') לצורך העלות כל התעודות באמצעותן החבר יפנה לחברים אחרים עבור פרויקט ניוד מידע
- **ייזום פניה ל API ע"פ הצורך** (תעודה חדשה, סיום תוקף תעודה וכו')

דרישות פיתוח

- מסר ב json
- מסר חתום ע"י תעודה של החבר (תעודת upload)
- פניה לתשתית NTN באמצעות תעודת mTLS
- תעודות שמועלות מכילות את ה public key ולא private key

[memberCert](#)

פיתוח נדרש

- פיתוח פניה ל API "הורדת תעודות" מתוך client (טופס, מערכת, תהליך וכדו')
- ייזום פניה כל 5 דקות 24/7 (מצריך תהליך אוטומטי)
- פעולות נדרשות :

1. הורדת קובץ תעודות כל חברי התשתית המתקבל מ presigned url
ה- API מחזיר תמונה עדכנית של תעודות כל חברי תשתית NTN
2. הסרת תעודות ישנות מתשתית הארגון
3. התקנת תעודות חדשות בתשתית הארגון

דרישות פיתוח

- מסר ב json
- מסר חתום ע"י תעודה של תשתית NTN (תעודת download)
- פניה לתשתית NTN באמצעות תעודת mtls

[ntnManifest](https://ntnmanifest.com)

פונקציות עיקריות

- הורדת תעודות של תשתית NTN

1. תעודת TA לצורך אימות תעודות tls ו download
2. תעודת MTLS לצורך הפעלת ה APIs של תשתית NTN
3. תעודת download לצורך אימות חתימת מסר של ממשק הורדת תעודות

- העלאת תעודות של חבר בתשתית

1. תעודת CA לצורך אימות תעודות tls ו upload במקרה של תעודות self signed
2. תעודת MTLS לצורך הפעלת ה APIs של תשתית NTN
3. תעודת upload לצורך אימות חתימת מסר של ממשק העלאת תעודות

ארכיטקטורה

הארגון מחזיק תעודה דיגיטלית (Certificate) שהונפקה על ידי גוף מאשר (CA) ונרשמה במאגר האמון הלאומי (NTN). התעודה כוללת מפתח ציבורי, והארגון שומר אצלו את המפתח הפרטי התואם.



יצירת – JWT Assertion הארגון יוצר מסמך חתום דיגיטלית (JWT) המהווה הוכחת זהות. החתימה נעשית באמצעות המפתח הפרטי של הארגון.



פתיחת חיבור מאובטח – (mTLS) הארגון ומערכת PCM מקיימים תקשורת הדדית מוצפנת, שבה כל צד מאמת את זהותו באמצעות התעודה הדיגיטלית שלו. ה־JWT נשלח בערוץ ה־mTLS למערכת PCM.



אימות במערכת – PCM המערכת שולפת מה־NTN את המידע הציבורי על הארגון (תעודה / מפתח ציבורי, מאמת את חתימת ה־JWT ומוודאת שהתעודה תקפה ולא בוטלה.



הנפקת Access Token – לאחר אימות מוצלח, המערכת מנפיקה לארגון אסימון גישה קצר טווח, המשמש אותו לקריאות עתידיות לממשקי ה־API של PCM למשל (FHIR תוקף הטוקן 30 שניות).



דוג' לקריאה למערכת באמצעות ה: JWT

POST "authorization_endpoint" ←
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&
client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer&
client_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9....&
scope=consent.read consent.write fhir.read

HTTP GET [PCM FHIR BASE]/.well-known/smart-configuration

Response:

```
{  
  "authorization_endpoint": "[PCM AUTHORIZATION  
BASE]/authorize",  
  "token_endpoint": "[PCM AUTHORIZATION  
BASE]/token",  
}
```

דוג' לתגובה של ה PCM עם token barrear

```
{  
  "access_token": "eyJraWQiOiJxMjM0NTYiLCJhbGciOiJSUzI1NiJ9...",  
  "token_type": "Bearer",  
  "expires_in": 30,  
  "scope": "consent.read consent.write fhir.read"  
}
```

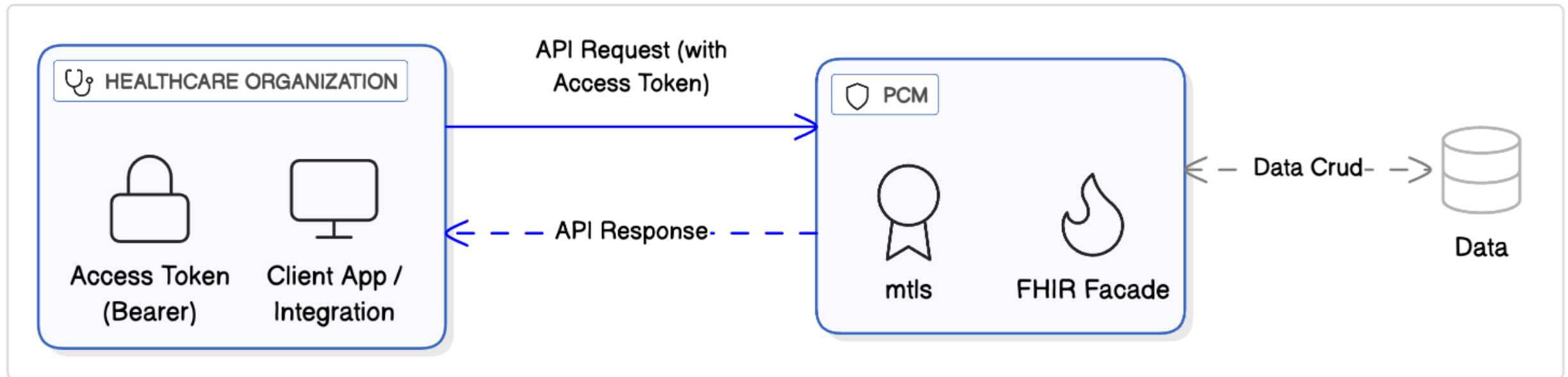
.

דוג' לקריאה אחרי קבלת הטוקן:

GET <https://pcm.gov.il/fhir/Consent/>"`consent-id`"

Authorization: Bearer <access_token>

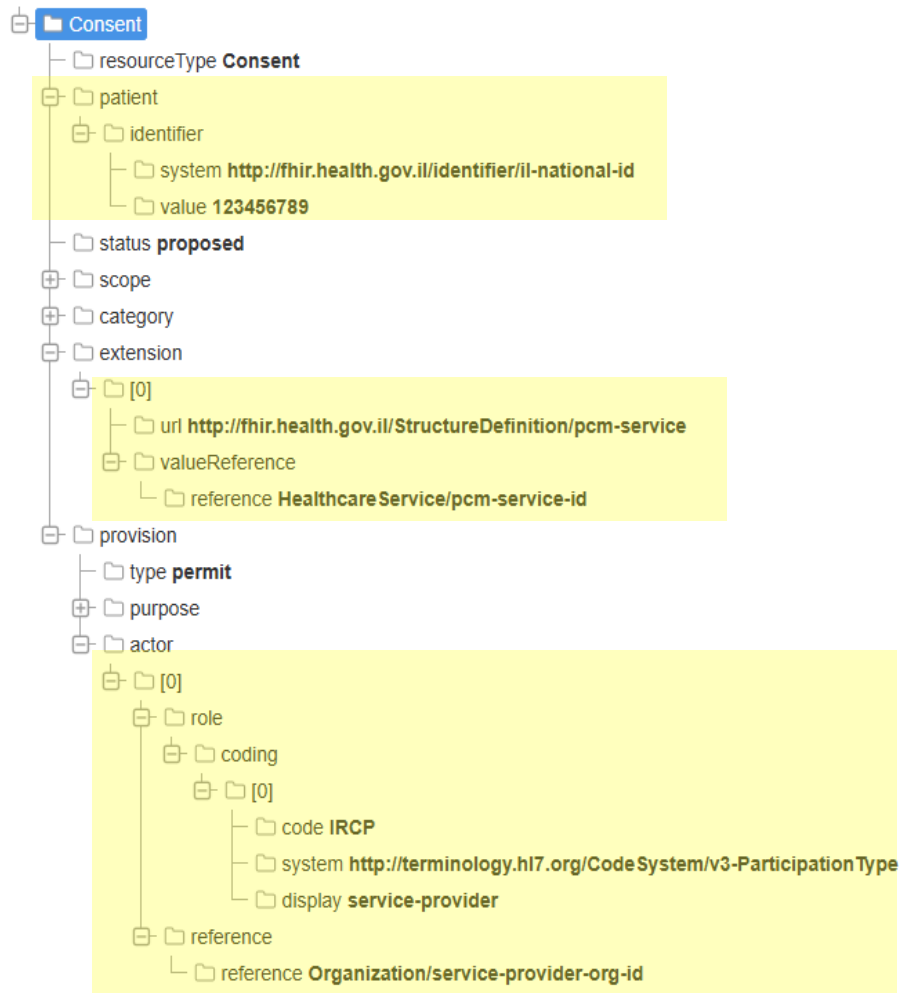
Accept: application/fhir+json



Example partial PCM access flow for service providers

Submit request for patient consent

Generate Consent resource



```
{
  "resourceType": "Consent",
  "patient": {
    "identifier": {
      "system": "http://fhir.health.gov.il/identifier/il-national-id",
      "value": "123456789"
    }
  },
  "status": "proposed",
  "scope": {
    "coding": [
      {
        "code": "patient-privacy",
        "system": "http://terminology.hl7.org/CodeSystem/consentscope",
        "display": "Privacy Consent"
      }
    ]
  },
  "category": [
    {
      "coding": [
        {
          "code": "INFA",
          "system": "http://terminology.hl7.org/CodeSystem/v3-ActCode",
          "display": "information access"
        }
      ]
    }
  ],
  "extension": [
    {
      "url": "http://fhir.health.gov.il/StructureDefinition/pcm-service",
      "valueReference": {
        "reference": "HealthcareService/pcm-service-id"
      }
    }
  ],
  "provision": {
    "type": "permit",
    "purpose": [
      {
        "code": "TREAT",
        "system": "http://terminology.hl7.org/CodeSystem/v3-ActReason"
      }
    ]
  },
  "actor": [
    {
      "role": {
        "coding": [
          {
            "code": "IRCP",
            "system": "http://terminology.hl7.org/CodeSystem/v3-ParticipationType",
            "display": "service-provider"
          }
        ]
      },
      "reference": {

```


Submit request for patient consent

Send request to PCM

1. HTTP POST Consent resource to `[PCM FHIR BASE]/Consent` endpoint using bearer token received at previous step, get back resource with ID

- Response:

```
{
  "resourceType": "Consent",
  "id": "resource-id-12345",
  "meta": {
    "versionId": "1",
    "lastUpdated": "2025-11-09T11:38:53.845+00:00",
    ...
  }
}
```

Consent request approval

- Contact patient somehow, tell them to open PCM and approve the request

Check Consent status

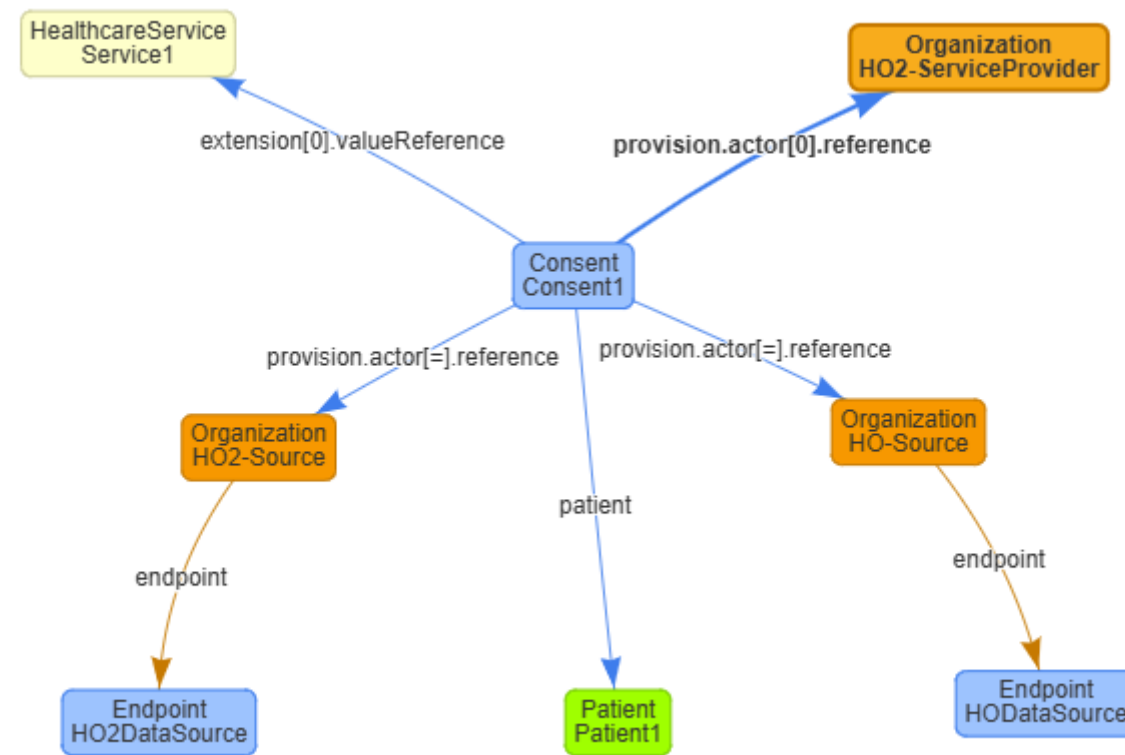
Request

1. Request Consent resource (using bearer token) with status and endpoints via **HTTP**

GET [PCM FHIR BASE]/Consent?_id=resource-id-12345&_include=Consent:actor&_include:iterate=Organization:endpoint&_include:iterate=Organization:partof

Check Consent status

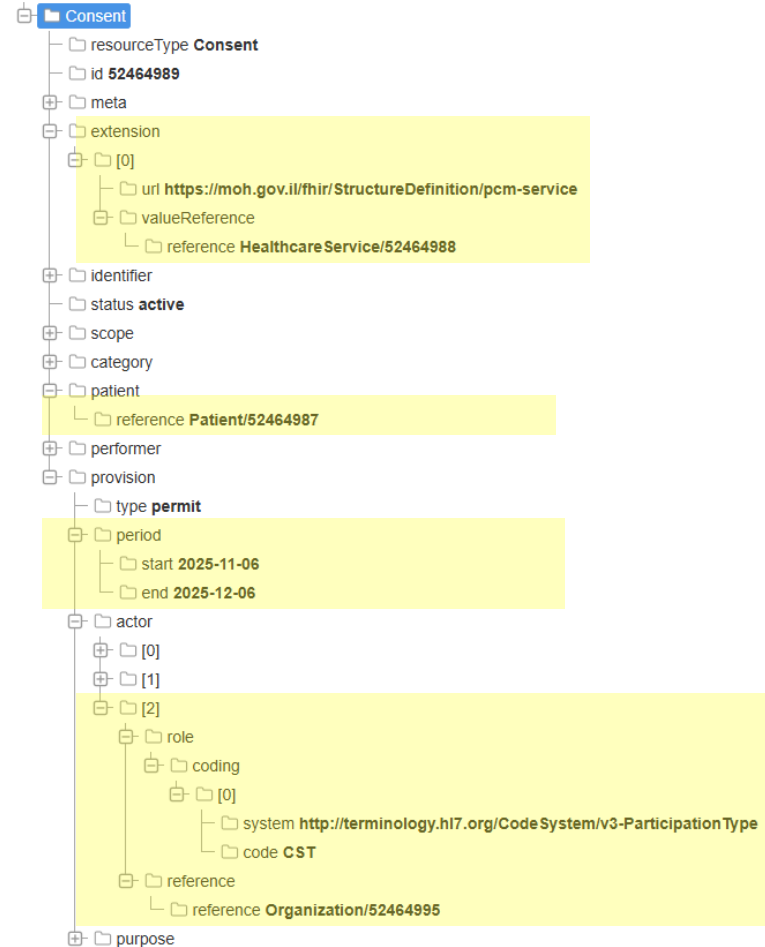
Response – data model



Check Consent status

Response - Consent

Consent Id: 52464989
Organization Id: 52464995
Organization Id: 52464991
Organization Id: 52464992
Organization Id: 52464993
Endpoint Id: 52464994
Organization Id: 52464985
Endpoint Id: 52464986

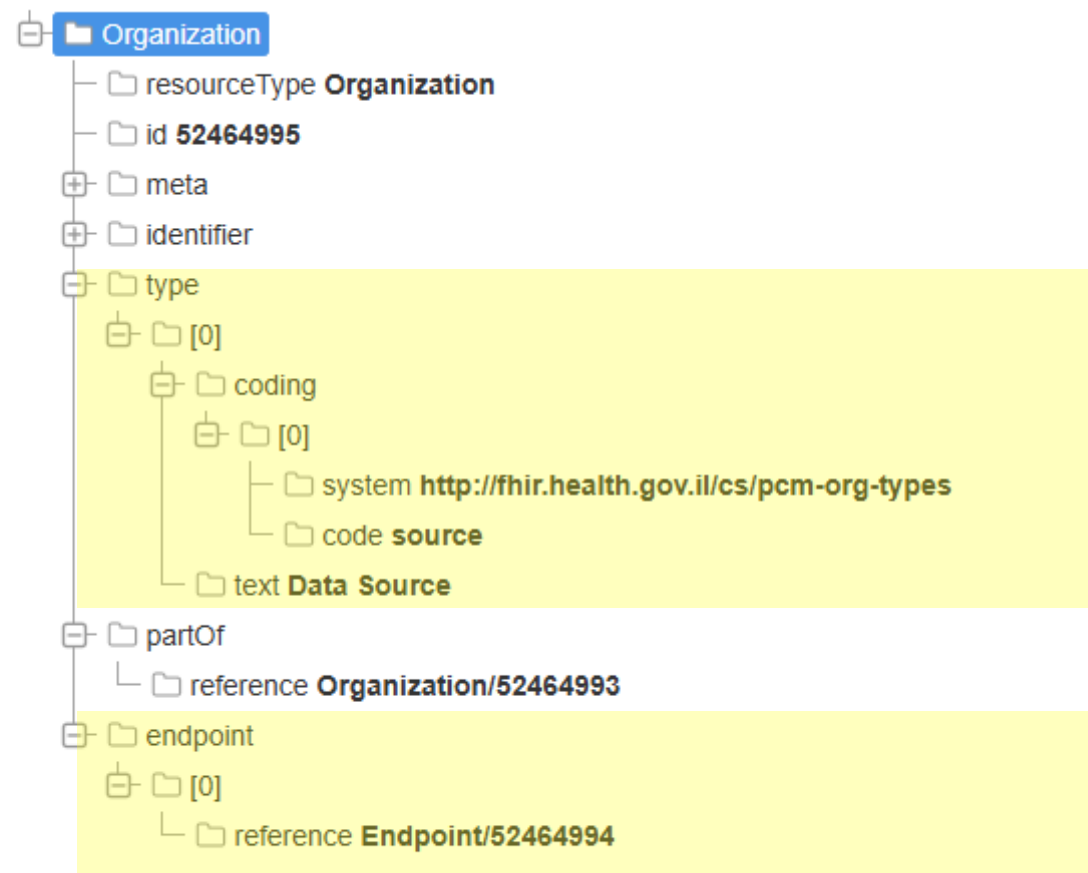


```
{
  "resourceType": "Bundle",
  "id": "3efd462e-0511-4d89-acd7-5b47c735cb95",
  "meta": {
    "lastUpdated": "2025-11-09T11:46:31.740+00:00"
  },
  "type": "searchset",
  "total": 1,
  "link": [ {
    "relation": "self",
    "url": "[PCM FHIR BASE]/Consent?_id=resource-id-12345&_include=Consent:actor&_include:iterate=Organization:endpoint&_include:iterate=Organization:partof"
  } ],
  "entry": [ {
    "fullUrl": "https://hapi.fhir.org/baseR4/Consent/resource-id-12345",
    "resource": {
      "resourceType": "Consent",
      "id": "resource-id-12345",
      "meta": {
        "versionId": "1",
        "lastUpdated": "2025-11-09T10:14:31.705+00:00",
        "source": "#nW7htESi6Wshq6ZK"
      },
      "extension": [ {
        "url": "https://moh.gov.il/fhir/StructureDefinition/pcm-service",
        "valueReference": {
          "reference": "HealthcareService/pcm-service-id"
        }
      } ],
      "identifier": [ {
        "use": "official",
        "system": "http://pcm.test2/identifiers",
        "value": "consent1"
      } ],
      "status": "active",
      "scope": {
        "coding": [ {
          "system": "http://terminology.hl7.org/CodeSystem/consentscope",
          "code": "patient-privacy",
          "display": "Privacy Consent"
        } ]
      },
      "category": [ {
        "coding": [ {
          "system": "http://terminology.hl7.org/CodeSystem/v3-ActCode",
          "code": "INFA",
          "display": "information access"
        } ]
      } ],
      "patient": {
        "reference": "Patient/52464987"
      },
      "performer": [ {
        "reference": "Patient/52464987"
      } ],
      "provision": {
```

Check Consent status

Response - Organization

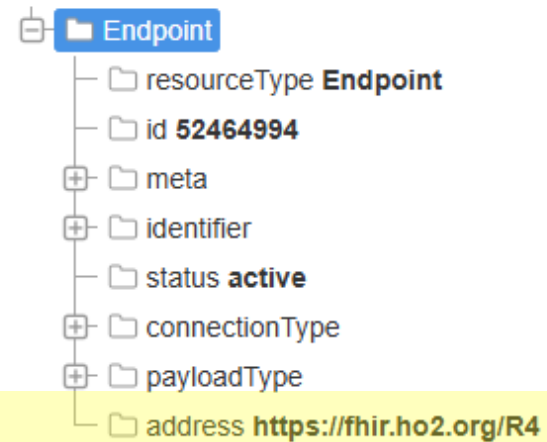
Consent <i>Id: 52464989</i>
Organization <i>Id: 52464995</i>
Organization <i>Id: 52464991</i>
Organization <i>Id: 52464992</i>
Organization <i>Id: 52464993</i>
Endpoint <i>Id: 52464994</i>
Organization <i>Id: 52464985</i>
Endpoint <i>Id: 52464986</i>



Check Consent status

Response - Endpoint

Consent <i>Id: 52464989</i>
Organization <i>Id: 52464995</i>
Organization <i>Id: 52464991</i>
Organization <i>Id: 52464992</i>
Organization <i>Id: 52464993</i>
Endpoint <i>Id: 52464994</i>
Organization <i>Id: 52464985</i>
Endpoint <i>Id: 52464986</i>



**Data Source FHIR
endpoint URL**

Get access tokens to data sources

- Steps 6-7

Data source

Request – service provider side

- (using bearer token from PCM)

HTTP GET [Data Source FHIR BASE]/Condition

Data source

Request – data source side

1. Recieve **HTTP GET** [Data Source FHIR BASE]/Condition with bearer token from PCM
2. Authenticate to PCM using NTN certificate and get **PCM access token**
3. With PCM access token as bearer do **HTTP POST** [PCM AUTHORIZATION BASE]/introspect sending access token from service provider

POST /introspect HTTP/1.1

Host: server.example.com

Accept: application/json

Content-Type: application/x-www-form-urlencoded

Authorization: Bearer 23410913-abewfq.123483

token=2YotnFZFEjr1zCsicMWpAA

PCM access token

Service Provider access token

Data source

Request – data source side (introspection)

```
{
  "active": true,
  "patient": "http://fhir.health.gov.il/identifier/il-national-id|000000018",
  "aud": "https://fhir.maccabi4u.co.il/R4",
  "iss": "https://pcm.fhir.health.gov.il/",
  "token_type": "bearer",
  "scope":
    "patient/Encounter.rs?_security=http://fhir.health.gov.il/cs/hdp-information-buckets|EncounterInformation&date=ge2024-01-01",
  "client_id": "http://pcm.fhir.health.gov.il/organization/633",
  "expires_in": 3600,
  "iat": 1633532014,
  "exp": 1633535614,
  "jti": "550e8400-e29b-41d4-a716-446655440000",
  "intent": "http://pcm.fhir.health.gov.il/healthcareservice/269321"
}
```

**Replace with
internal logical id**

**Server enforces
scopes**

Data source Response

- Data source side
 - Enforce patient context and scopes received via introspection and return data according to FHIR REST API query
- Service provider side
 - Receive and process data

המשך הפעילות

- היערכות בתוכנית העבודה ל 2026 לפיתוח ואינטגרציה מול ה NTN , PCM במקור מידע / נותן שירות- נובמבר 25
- פגישת design review לפיתוח MVP1 – דצמבר 25
- פגישת אפיון תהליך הזדהות מול הקופות וקבלת מידע על חוסים – ינואר 26
- קטלוג שירותים רפואיים- ינואר 26
- אינטגרציה לתכולות MVP1 – מרץ 26

FHIR® IL by 8400



משרד
הבריאות
לחיים בריאים יותר



תודה רבה!