PCM
Patient Consent Manager

הכנה לאינטגרציה MVP1 – מקור מידע

19.3.26

מטרת המפגש ואג'נדה

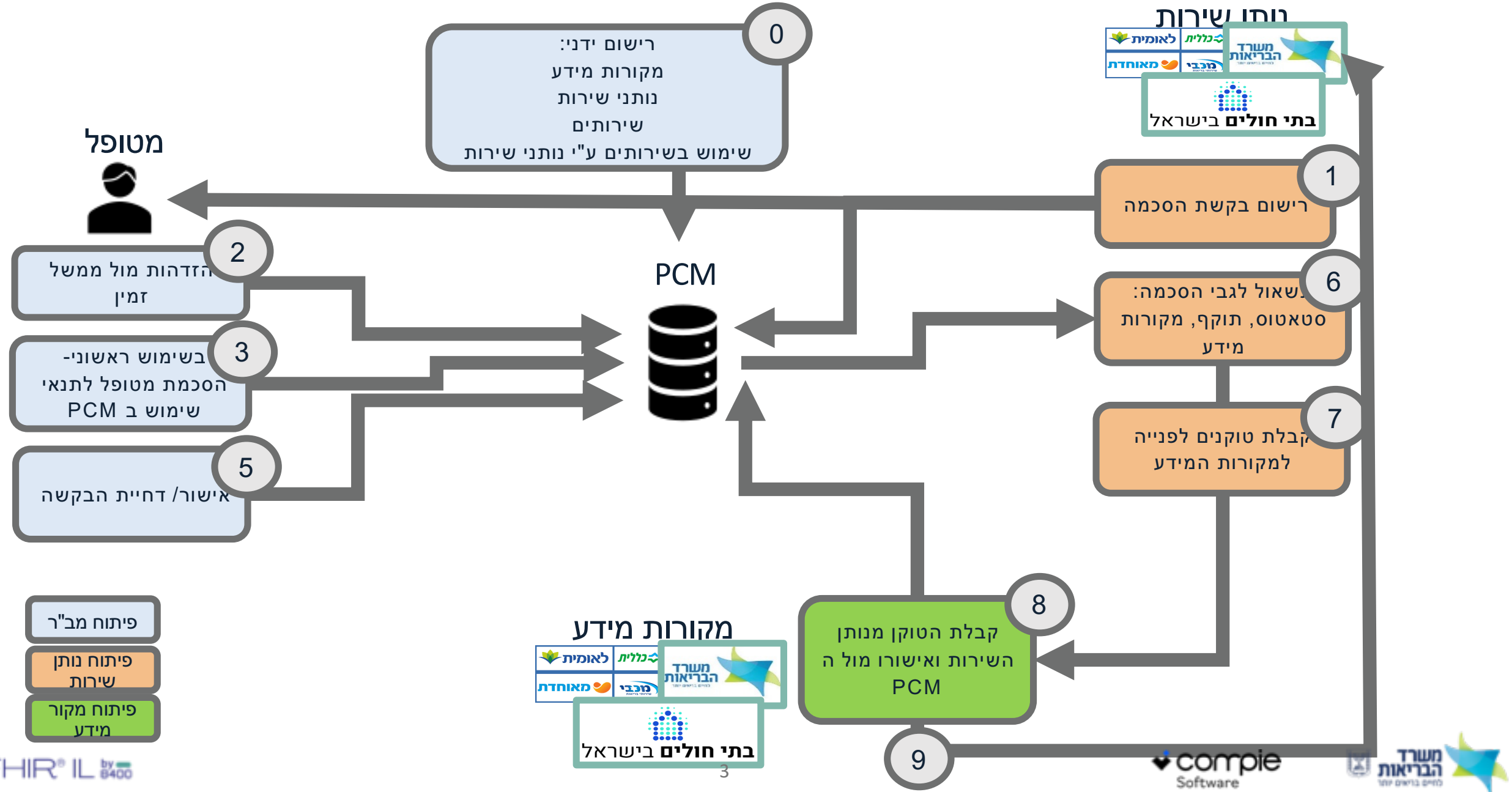
- **מטרת המפגש:**

הכנה לאינטגרציה מול ה PCM **בכובע של מקור מידע**

אג'נדה:

- הכנות נדרשות מצד הארגון (מקור מידע)
- הכנות נדרשות מצד מב"ר
- מעבר על התרחישים שיבוצעו באינטגרציה
- מדדי הצלחה לאינטגרציה
- צעדים להמשך
- תכולות שלב 2
- השתתפות בסקר 

תבולות MVP1


0
רישום ידני:
מקורות מידע
נותני שירות
שירותים
שימוש בשירותים ע"י נותני שירות
נותני שירות
כללית
לאומית
מאוחדת
מכבי
משרד הבריאות
בתי חולים בישראל
מטופל
1
רישום בקשת הסכמה
2
הזדהות מול ממשל זמין
PCM
3
בשימוש ראשוני- הסכמת מטופל לתנאי שימוש ב PCM
6
שאול לגבי הסכמה:
סטאטוס, תוקף, מקורות מידע
7
קבלת טוקנים לפנייה למקורות המידע
5
אישור/ דחיית הבקשה
8
קבלת הטוקן מנותן השירות ואישורו מול ה PCM
מקורות מידע
כללית
לאומית
מאוחדת
מכבי
משרד הבריאות
בתי חולים בישראל
9
פיתוח מב"ר
פיתוח נותן שירות
פיתוח מקור מידע

הכנות בצד מקור המידע

- **הכנת תשתית MTLS**
  - שליחת CSR למב"ר על פי ההנחיות
  - הטמעת ה signed certificate וה CA Certificate של מב"ר

- **יוקם צוות תמיכה רוחבי שיסייע לארגונים להטמיע את תשתית ה MTLS.**

תיקבע פגישה עם כל ארגון בנפרד, לפגישה יש לצרף את בעלי התפקידים הבאים מהארגון:

מנהל פרויקט ניוד מידע

איש סיסטם שאחראי על תשתית PKI

איש אבט"מ

1. Subject Information (Distinguished Name — DN)

Field	Required?	Example	Notes
CN – Common Name	Yes	https://TestOrgPCM.TLS.gov.il	For TLS server: hostname / FQDN.
O – Organization	Yes	Test Org	Legal organization name.
OU – Organizational Unit	Yes	Test Org ICT	Internal grouping.
C – Country	Yes	IL	ISO-3166 2-letter code.
L – Locality/City	Yes	Tel Aviv	

2. Subject Alternative Names (SAN)

Required types:

- **DNS Names**:
  - https://TestOrgPCM.TLS.gov.il.gov.il
  - https://api.TestOrgPCM.TLS.gov.il.gov.il

Note: CN is obsolete for hostname validation; SAN is authoritative.

3. Key Parameters

Parameter	Example	Notes
Key Algorithm	ECDSA P-256	Most common: RSA 2048/3072; ECDSA P-256/P-384.
Key Size / Curve	ECDSA SECP-256	Must match policy.
Key Usage (KU)	digitalSignature	Restricts operations allowed.
Extended Key Usage (EKU)	ServerAuth, clientAuth, Code signing	Defines allowed certificate purposes.
Signature Hash Algorithm	SHA-256	

4. Certificate Policy Parameters

Parameter	Purpose
Basic Constraints	CA: False
Path Length Constraint	For intermediate CAs.
CRL Distribution Points (CDP)	http://cdp.TestOrg.gov.il/crl
Authority Information Access (AIA)	CA-TestOrg.
Certificate Policies (OID)	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.3
OCSP Must-Staple	False

5. Validity Parameters

Parameter	Notes
Requested expiration	3 years. Public TLS max is 397 days.
Start date	Actual Date
Renewal requirements	Automated via ACME or scripts.

6. CSR Attributes

Generate a **CSR (Certificate Signing Request)** with:

1.Subject DN
2.SAN list
3.Public key
4.Key size/curve

Verify and issue the certificate using the CSR.

7. Operational Metadata for the System

Metadata	Example / Purpose
System name / service name	"NTN"
Environment	Dev
Contact person	Israel Israeli (System Security Responsible Person)
NTN	NTN Local Host, Data Sharing Local Host
Private key storage	Local file, Secrets Manager
Automation requirements	ACME

נוהל הנפקת תעודה

הכנות בצד מקור המידע

- **הגדרת מטופל סינתטי:**

(מזהה "1") במערכות הארגוניות התואם להגדרות ה-PCM

בהתאם למסמך דרישות טכנולוגיות (סעיף 3.10) - לינק למסמך

Field	1st Synthetic Patient
Patient.identifier.system	http://fhir.health.gov.il/identifier/il-hdp-test-id
Patient.identifier.value	1
Patient.name.given	Israel
Patient.name.family	Israelov
Patient.meta.security.system	http://terminology.hl7.org/CodeSystem/v3-ActReason
Patient.meta.security.code	HTEST

- **סביבת עבודה:** וידוא מוכנות שרת ה-FHIR הארגוני (במידה וקיים) לקבלת שאילתות וביצוע Parse לנתונים.

- **שליחה למב"ר:** FHIR Endpoint – Endpoint חיצוני שחשוף לאינטרנט

הכנות בצד מב"ר

- **הגדרות ארגונים:**
  - הקמת הארגונים במקורות מידע במערכת
  - הגדרת ארגונים רלוונטיים בנותן שירות (לצורך האינטגרציה: מב"ר).

- **הגדרת מטופל פיקטיבי:**
  - הגדרת מטופל פיקטיבי "1"
  - אבלוס טבלת מקורות מידע המחזיקים מידע על מטופל "1"

- **הגדרת שירותים:**
  - שירות עם Scope פשוט - "patient/Patient.r"
  - שירות עם Scope מורכב -

"patient/Patient.r?_security=http://fhir.health.gov.il/cs/hdp-information-buckets|patientDemographics"

- **רישום נותן שירות לשימוש בשירותים :** רישום מב"ר בנותן שירות לשני השירותים.

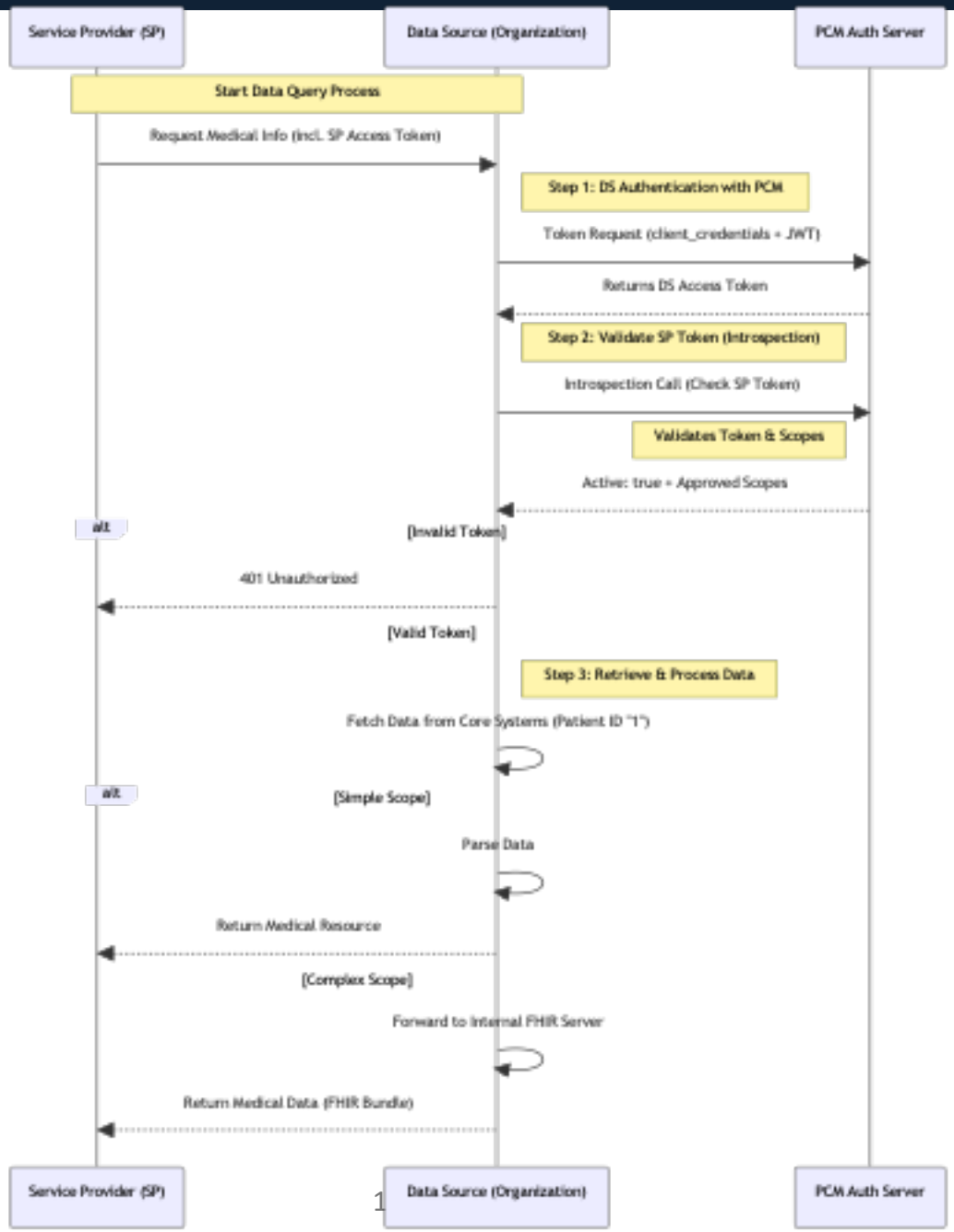
- **הקמת CA מרכזי והנפקת תעודה**

תרחישים

תרחיש אינטגרציה - אימות טוקן ושליפת מידע
בתרחיש זה, הארגון במקור מידע נדרש להגיב לפנייה של נותן שירות המבקש מידע:

- **הזדהות:** הארגון מבצע הזדהות מול ה-PCM (באמצעות Client Credentials) לקבלת Access Token.
- **אינטרוספקציה (Introspection):** המקור מקבל טוקן מנותן השירות ופונה ל-PCM לוודא את תקינותו והיקף ההרשאות (Scopes) שבו.
- **עיבוד הבקשה:** במידה והטוקן תקין, המקור שואב את המידע מהמערכות הפנימיות בהתאם לבקשה.
- **העברת מידע:** החזרת המידע הרפואי לנותן השירות (עבור Scope פשוט).

תרחישים


Service Provider (SP)
Data Source (Organization)
PCM Auth Server
Start Data Query Process
Request Medical Info (incl. SP Access Token)
Step 1: DS Authentication with PCM
Token Request (client_credentials + JWT)
Returns DS Access Token
Step 2: Validate SP Token (Introspection)
Introspection Call (Check SP Token)
Validates Token & Scopes
Active: true + Approved Scopes
alt
[Invalid Token]
401 Unauthorized
[Valid Token]
Step 3: Retrieve & Process Data
Fetch Data from Core Systems (Patient ID "1")
alt
[Simple Scope]
Parse Data
Return Medical Resource
[Complex Scope]
Forward to Internal FHIR Server
Return Medical Data (FHIR Bundle)
Service Provider (SP)
Data Source (Organization)
PCM Auth Server

מדדי הצלחה – מקור מידע

מדדי הצלחה לארגון כמקור מידע

האינטגרציה תיחשב כהצלחה בהתקיים לפחות שני המדדים הראשונים:

- **הזדהות: ביצוע תהליך Authentication מול ה-PCM וקבלת טוקן ללא שגיאות.**
- **אימות הרשאות: פנייה מוצלחת ל-Introspection Endpoint וקבלת תשובה ולידית על טוקן של נותן שירות.**
- **טיפול ב-Scope פשוט:** ביצוע Parse מוצלח לתשובת ה-Introspection, העברת המידע לשרת ה FHIR הארגוני והחזרת המידע הנדרש למב"ר בנותן השירות.
- **טיפול ב-Scope מורכב:** ביצוע Parse מוצלח לתשובת ה-Introspection והעברה תקינה של המידע לשרת ה-FHIR הארגוני.

צעדים להמשך

תיאום פגישות אינטגרציה מול כל ארגון בנפרד (אפריל-יולי 2026) - מירי ועדי מול מנהל ניוד מידע בארגון**

- פגישת MTLS
  - **מטרה**: ביצוע handshake של התעודות
  - **משתתפים נדרשים מצד הארגון**: מנהל פרויקט, איש סיסטם, איש אבטחת מידע

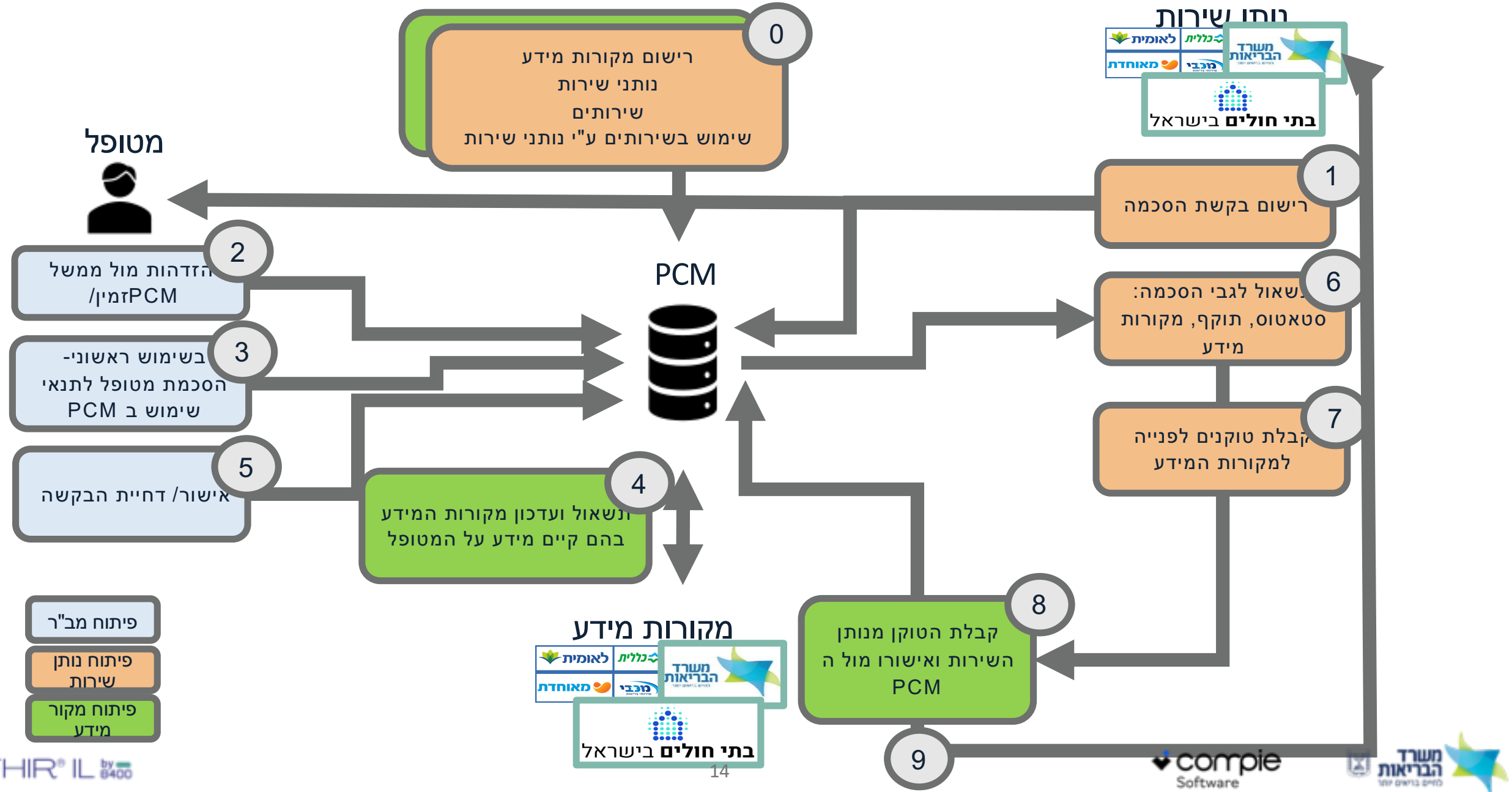
- פגישת ביצוע תרחישי אינגרציה – כחצי יום עבודה
  - **מטרה:** הרצה מקצה לקצה של התרחישים (הזדהות, אינטרוספקציה ושליפת מידע) בסביבת הבדיקות.
  - **משתתפים נדרשים:** מפתח Backend/FHIR, איש אבטחת מידע/תשתיות, ומנהל פרויקט מטעם הארגון.

- **ביצוע הכנות ע"י הארגון**

- **פגישת הכנה לאינטגרציה בכובע של נותן שירות – לפנות למירי**

****עדי רביבו adi.revivo@moh.gov.il, מירי אלטשולר miri.altshuler@MOH.GOV.IL**

תבולות PCM


0
רישום מקורות מידע
נותני שירות
שירותים
שימוש בשירותים ע"י נותני שירות
נותני שירות
בתי חולים בישראל
מטופל
1
רישום בקשת הסכמה
2
הזדהות מול ממשל PCMזמין/
PCM
3
בשימוש ראשוני- הסכמת מטופל לתנאי שימוש ב PCM
6
נשאול לגבי הסכמה: סטאטוס, תוקף, מקורות מידע
7
קבלת טוקנים לפנייה למקורות המידע
5
אישור/ דחיית הבקשה
4
נשאול ועדכון מקורות המידע בהם קיים מידע על המטופל
8
קבלת הטוקן מנותן השירות ואישורו מול ה PCM
9
מקורות מידע
בתי חולים בישראל
פיתוח מב"ר
פיתוח נותן שירות
פיתוח מקור מידע

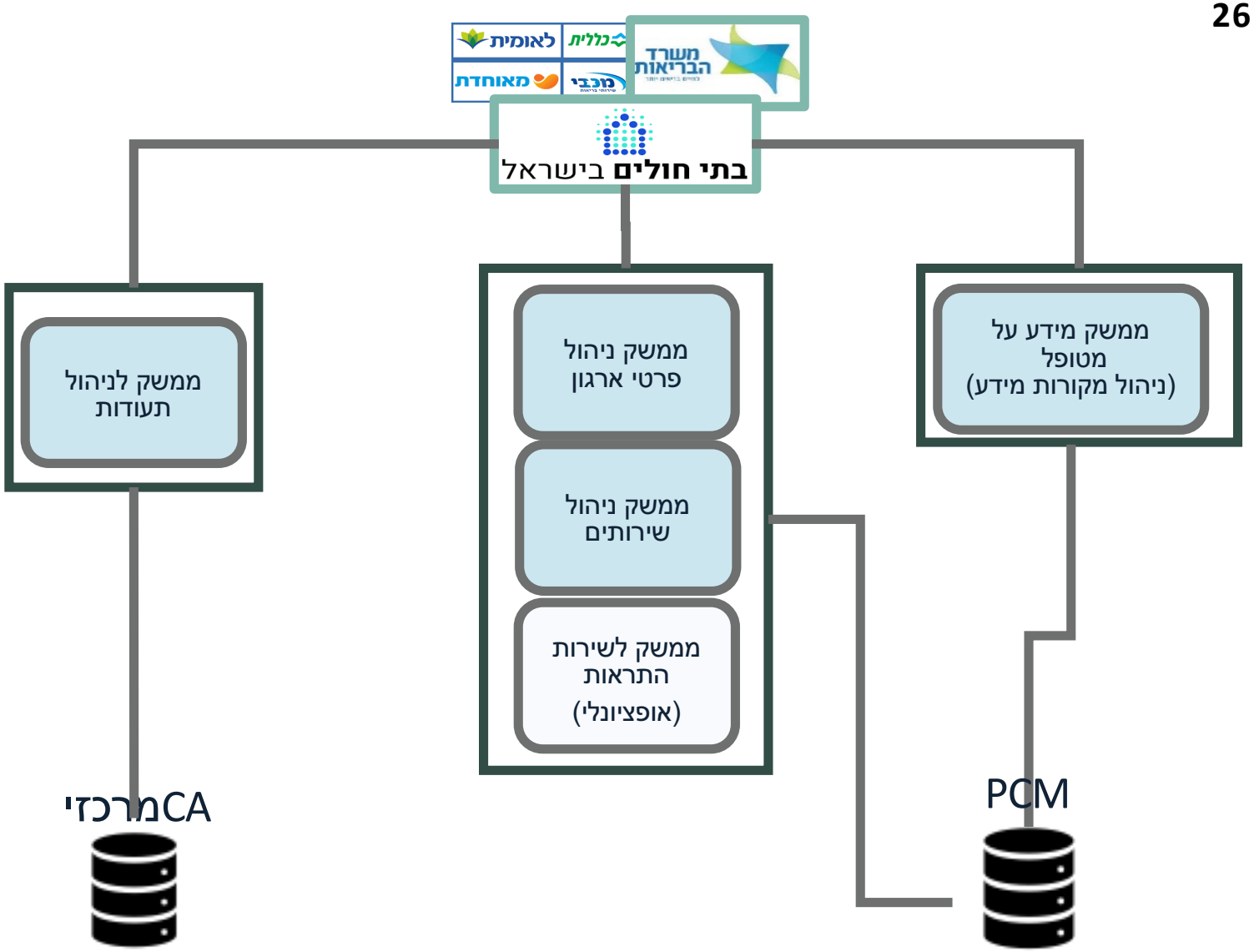
תכולות שלב 2 - מקור מידע

אינטגרציה החל מנובמבר 26, DR יתקיים ב 26.5.26

מקור מידע

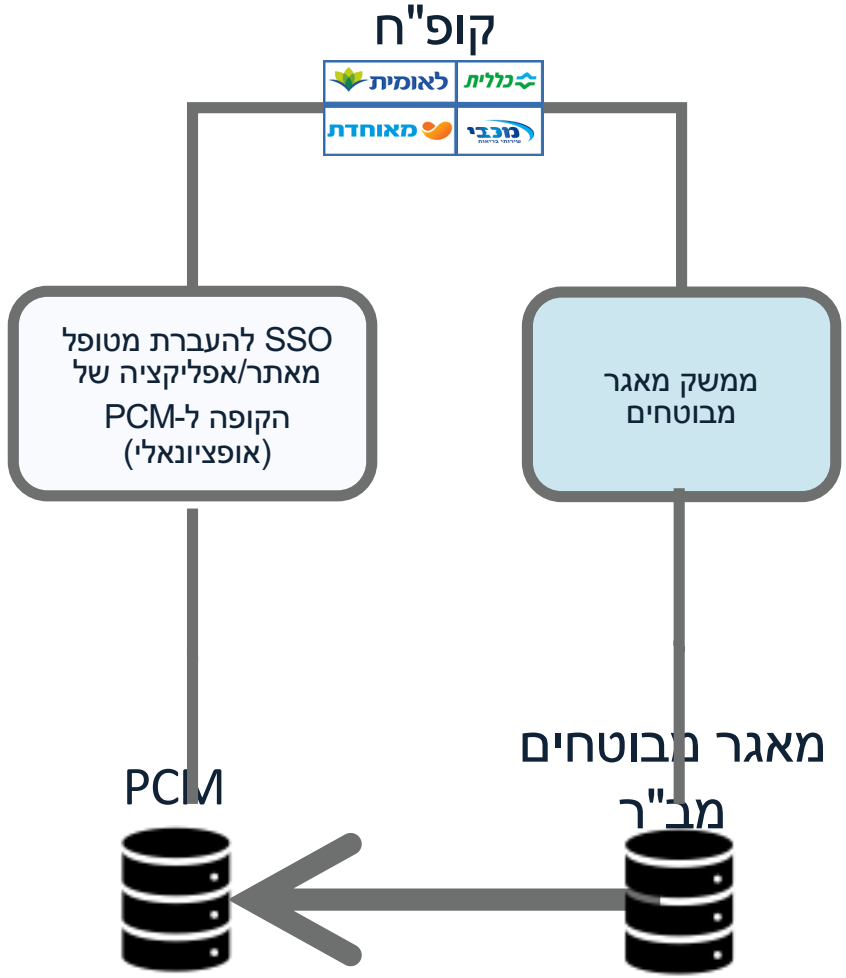
- **ממשק ניהול מידע על מטופלים (4)**
- **CA מרכזי - עדכונים**

- ממשק ניהול פרטי ארגון
- ממשק ניהול שירותים והסתייגויות
- אופציונאלי: רישום לשירות התראות – עבור שירותים



תכולות שלב 2 – קופת חולים

אינטגרציה החל מנובמבר 26, DR יתקיים 11.6.26

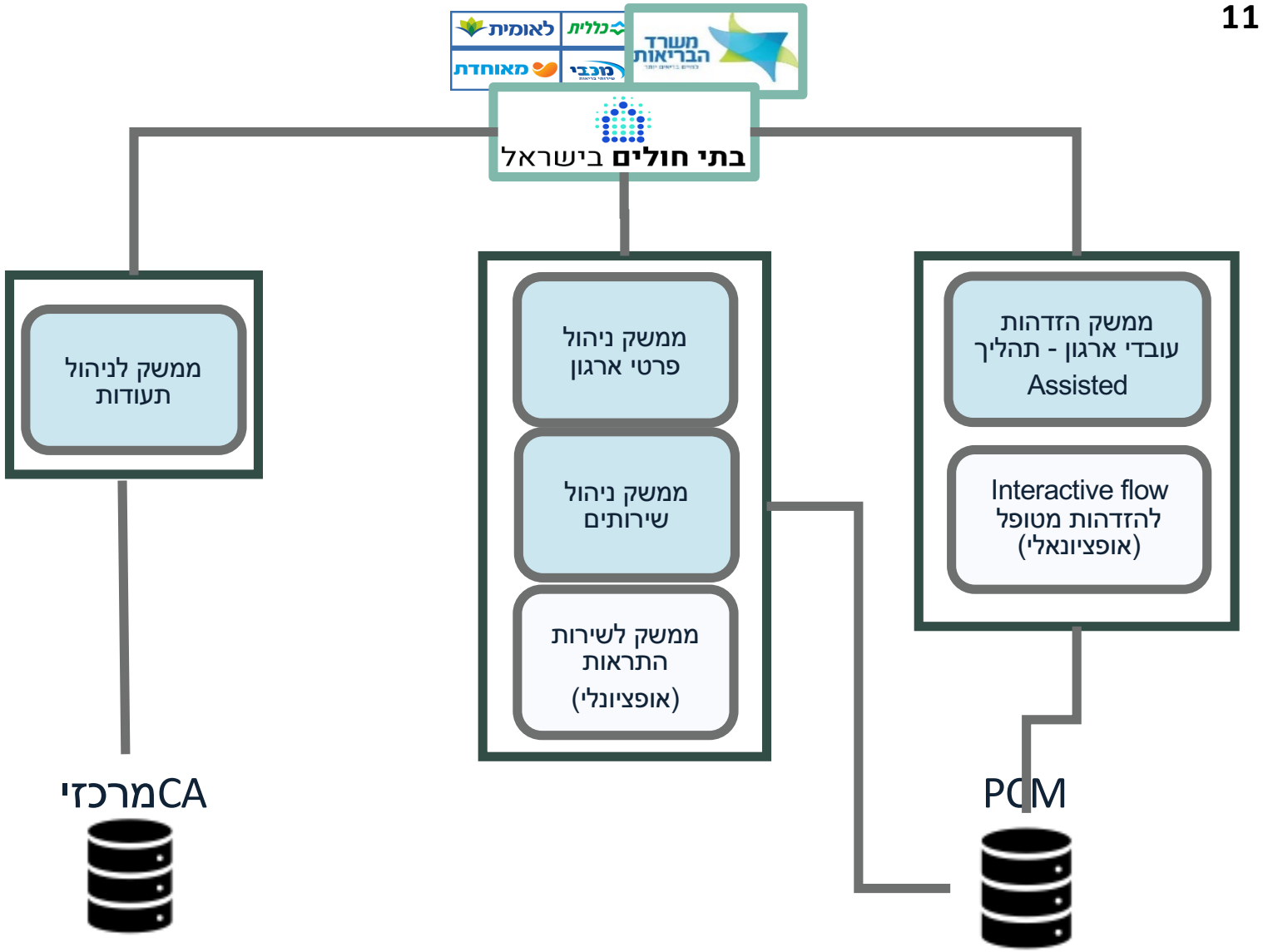


קופות חולים

- טיוב ממשק מאגר מבוטחים
- אופציונאלי:Re-direct מאתר הקופה ל PCM

תכולות שלב 2 – נותן שירות

אינטגרציה החל מנובמבר 26, DR יתקיים ב 11.6.26



נותן שירות

- ממשק הזדהות עובד ארגון עבור תהליך assisted – סיוע למטופלים לא דיגיטלים
- CA מרכזי - עדכונים
- ממשק ניהול פרטי ארגון
- ממשק ניהול שירותים והסתייגויות
- אופציונאלי: רישום לשירות התראות – עבור הסכמות
- אופציונאלי: interactive flow להזדהות מטופל

שם עברי ל PCM

ישלח סקר למנהלי ניוד מידע בארגונים- מי שמצביע משפיע!!!!

הסבמה

הסב"מ

מפתח

שיתוף

רשות

FHIR® IL by 8400

משרד הבריאות
לחיים בריאים יותר

תודה רבה!