



PATIENT CARE TEAM

Igal Vainer, Senior Director, Head of Enterprise Solutions Lab, EPAM Systems

Diagnostician



Nurse

Allergist



Surgeon



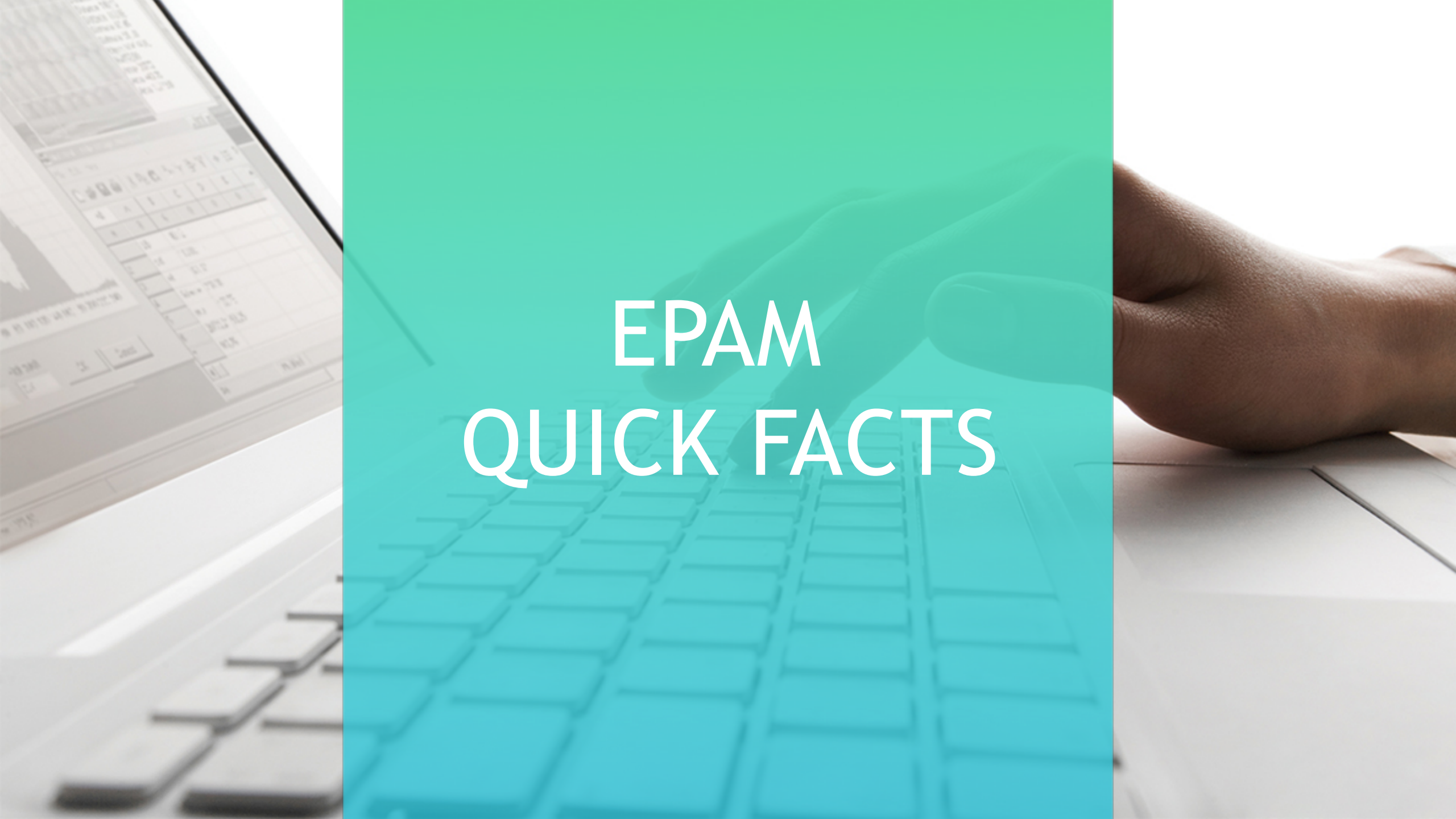
Patient

Dentist



Physician

SOLUTION OVERVIEW

A close-up photograph of a person's hand typing on a laptop keyboard. The image is partially obscured by a semi-transparent teal overlay that covers the center and right portions of the frame. The text 'EPAM QUICK FACTS' is centered within this teal area in a white, sans-serif font. The background shows the laptop screen with some data tables and the keyboard keys.

EPAM QUICK FACTS

EPAM OVERVIEW



Fast-growing, sizeable opportunity
in a global market



Deep talent pool of highly-skilled professionals
delivering solutions through best-in-class
engineering combined with strategy,
consulting and innovation services



Ability to deliver a broad range of
software engineering, digital
engagement, consulting and IT services
with a strong focus on innovative and
scalable software solutions



Industry solutions for Financial Services,
Travel and Consumer, Life Sciences and
Healthcare, Media and Entertainment, and
Software and Hi-Tech



Serving clients in over 25 countries across
North America, Europe, Asia, Australia
and Central and Eastern Europe



Proven ability to grow and sustain a
strong profitability model

WHO WE ARE

We are consultants, designers, architects and engineers who enable our customers to be competitive and disruptive in the marketplace through

INNOVATIVE TECHNOLOGY SOLUTIONS

while helping them to navigate successfully through multiple waves of technology change.

We help our customers be more competitive by delivering **solutions** through best-in-class engineering combined with strategy, design, consulting and innovation services.

We adopt a **global growth strategy**, thinking and acting like start-ups, working in multidisciplinary teams and delivering results. Relentlessly.

FACTS

FOUNDED IN

1993

US HEADQUARTERED
PUBLIC COMPANY
(NYSE:EPAM)FY 2016
REVENUE

\$1.16B

2017 REVENUE
GUIDANCE

\$1.4B

20+%

YOY CONSTANT
CURRENCY ORGANIC
GROWTH

REVENUE BY GEOGRAPHY*

59%

NORTH
AMERICA

35%

EUROPE

4%

CIS

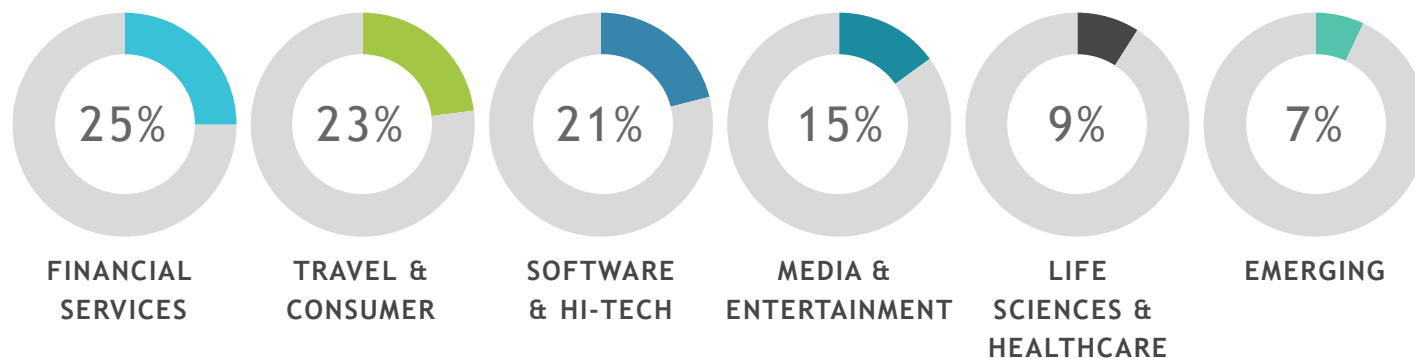
2%

APAC

25+ COUNTRIES

20,400+ Engineers | 24,000+ EPAMers

VERTICAL FOCUS*



SERVICE MIX

SOFTWARE ENGINEERING & PRODUCT/PLATFORM DEVELOPMENT

QA AND TEST AUTOMATION

MANAGED SERVICES

INFRASTRUCTURE & LICENSING

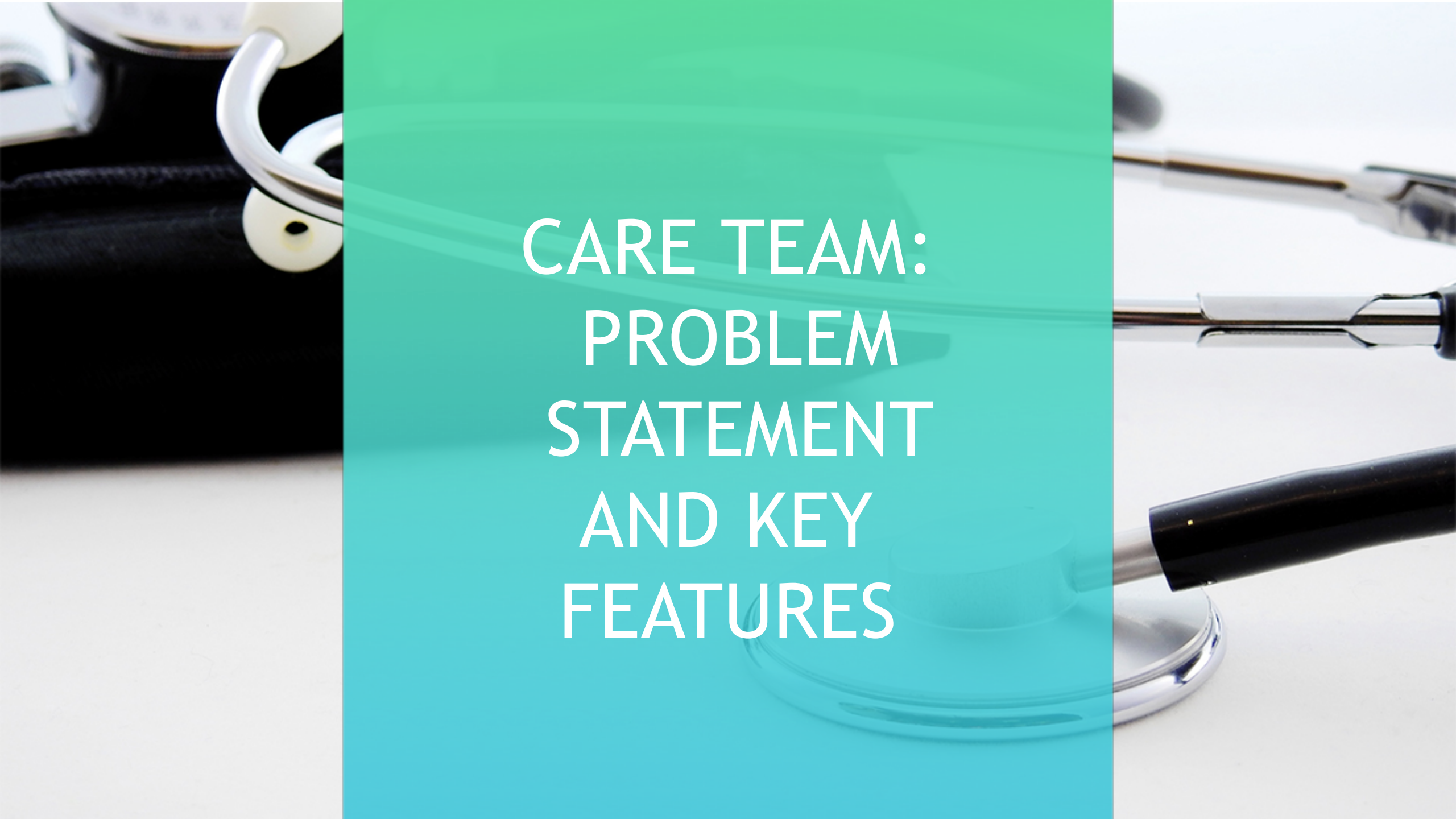
DIGITAL BUSINESS

PRODUCT ENGINEERING

MANAGED SERVICES

CONSULTING

* Data represents FY 2016 Earnings

The background of the slide is a blurred photograph of medical equipment. On the left, a white blood pressure cuff is visible. On the right, there are several medical pens or probes with silver and black components. A large, semi-transparent teal rectangle is centered over the image, containing the title text in white.

CARE TEAM: PROBLEM STATEMENT AND KEY FEATURES



Patients are usually unaware of the size of their care team and the names of the staff that are treating them



Hospital executives lack a comprehensive view of patient/staff interactions and resource utilization within the hospital

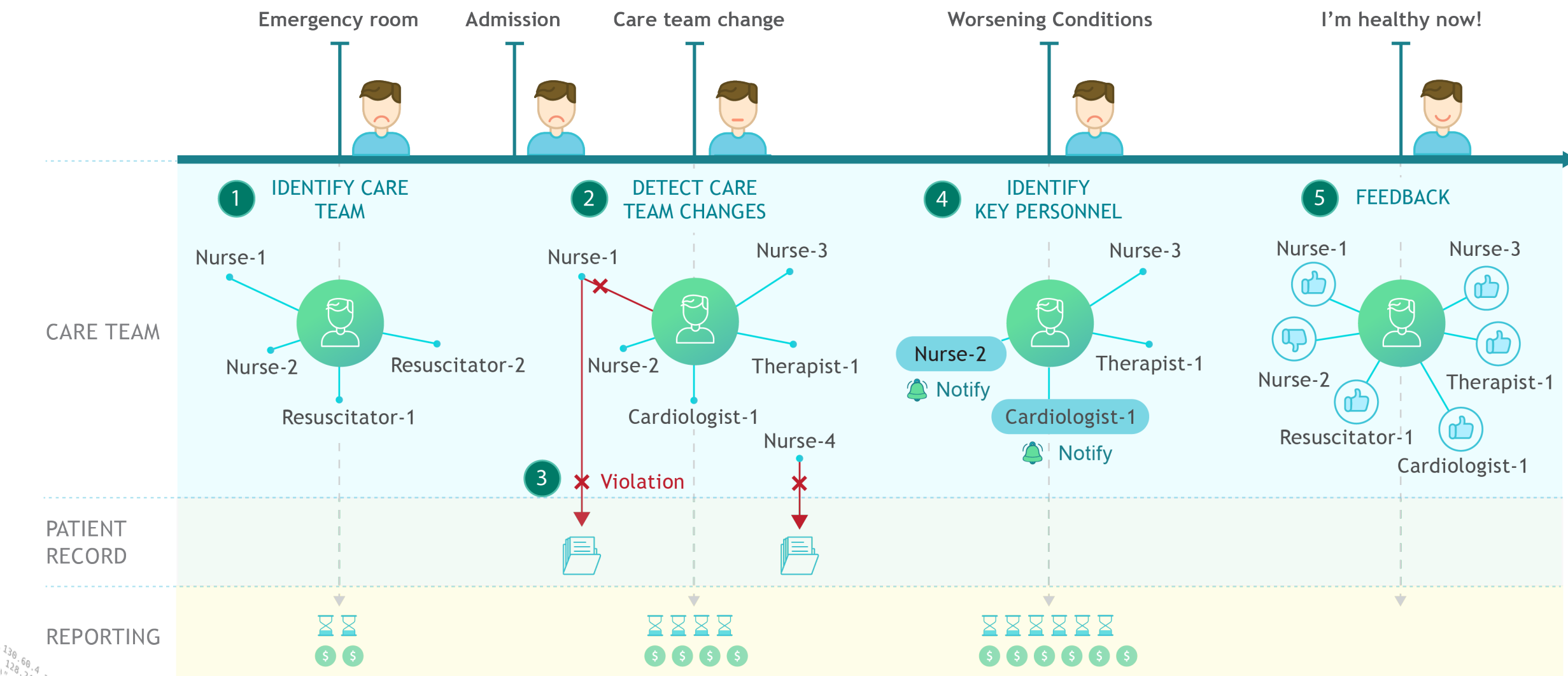


Clinical staff cannot quickly identify other relevant and available staff members in emergencies or for questions.



Compliance departments do not have a real-time view as to whether a staff member's patient record access is relevant to their job

IDEA OF CARETEAM



WHY WE CHOSE SPLUNK?



1. SINGLE TECHNOLOGY STACK

- Some HC vendors already use SPLUNK
- All-in-one solution



2. RAPID DEVELOPMENT

- Fast TTM (Time To Market)
- Relatively low cost of implementation



3. INTEGRABILITY

- Out-of-the-box integration patterns



4. MAINTAINABILITY & EXTENDIBILITY

- Out-of-the box mature maintenance solution
- Easy to maintain code.
- Fast and easy to extend functionality



5. SECURITY

- Out-of-the-box Authorization and Authentication mechanisms
- Support all modern and reliable approaches (SAML, LDAP, ..)



6. SCALABILITY

- Proven scalability approach on both indexer and search head sides



7. CUSTOMIZATION

- Deeply customizable on UI side

FACTS

Implementation Efforts

~300
man/days

Team of
6
people

- 2 Splunk developers
- UI developer
- UI designer
- BA
- Architect/DM

Time To Market

3.5 months

Healthcare
Domain

File Formats

ADT, ORM, CCD,
RTLS log files

Custom generators
to generate input data

4

user
roles

8

entries
(dashboards)



Jenkins

as an orchestration tool to build, deploy and
validate system on Splunk envs in 15 mins.

~20
lookups

Data-Driven Documents

BACKBONE.JS

Extensive
customization
on UI side

<2s response
time

3 search
heads

Full-functional application

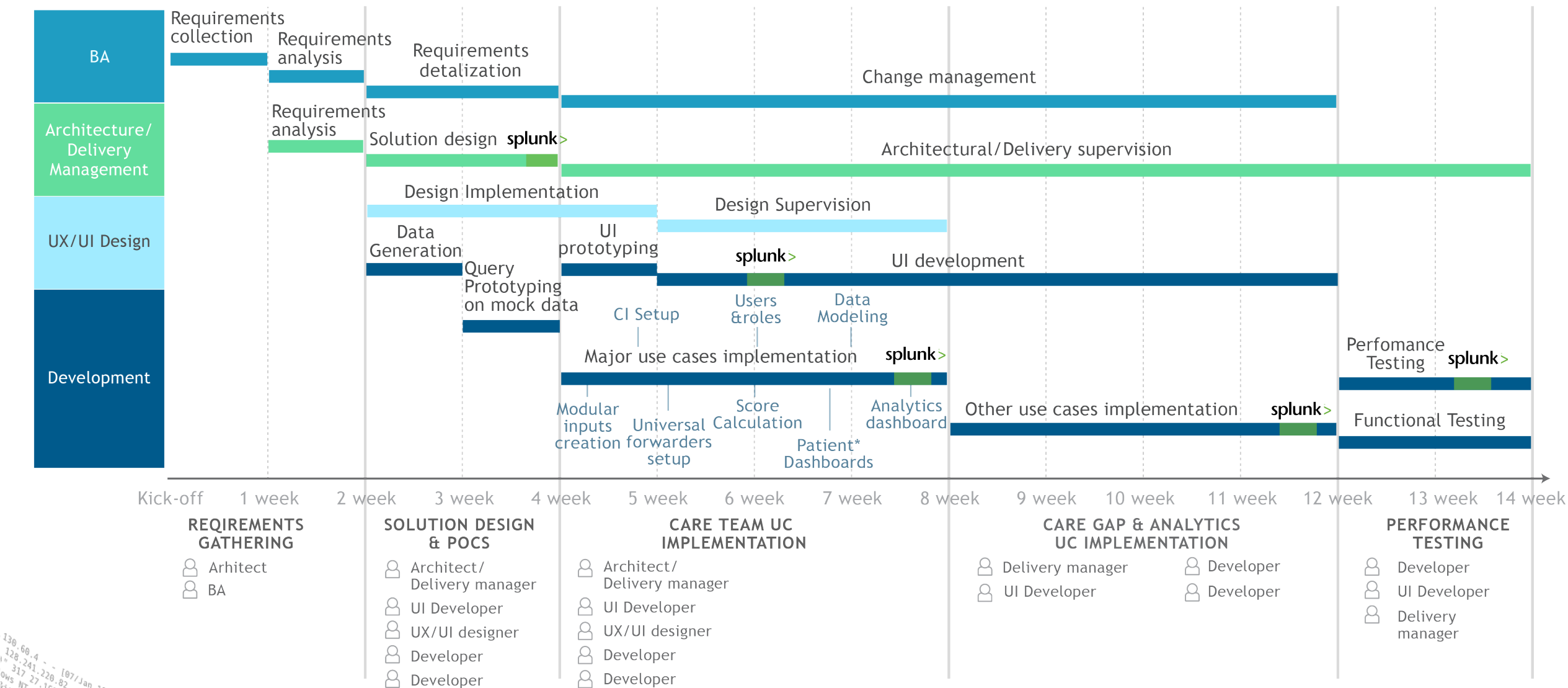
which is easy
to maintain
and extend.

PHI data masking.

Mutable (KV Store) and
Immutable (Index) data

>30
saved searches

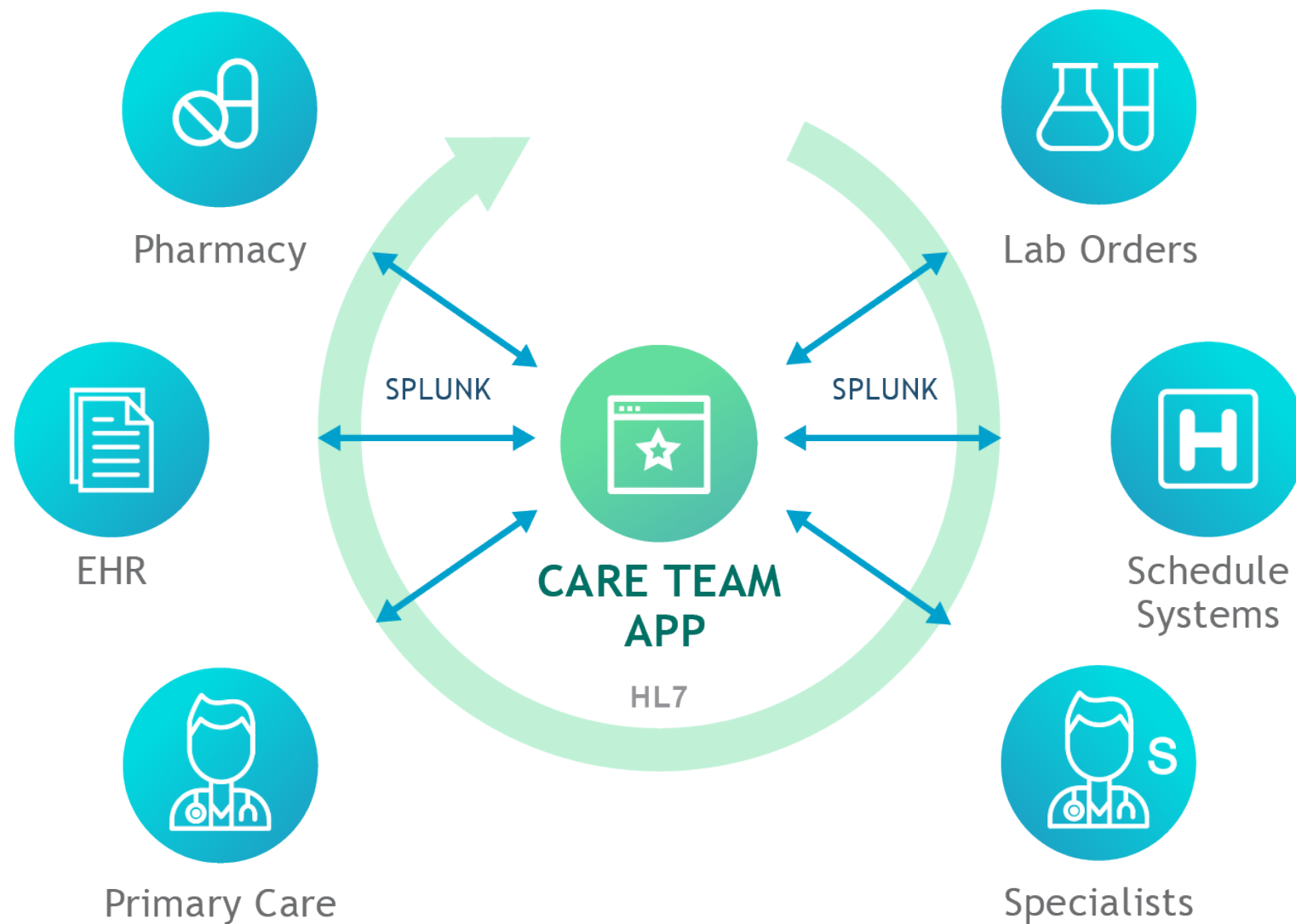
OUR APPROACH



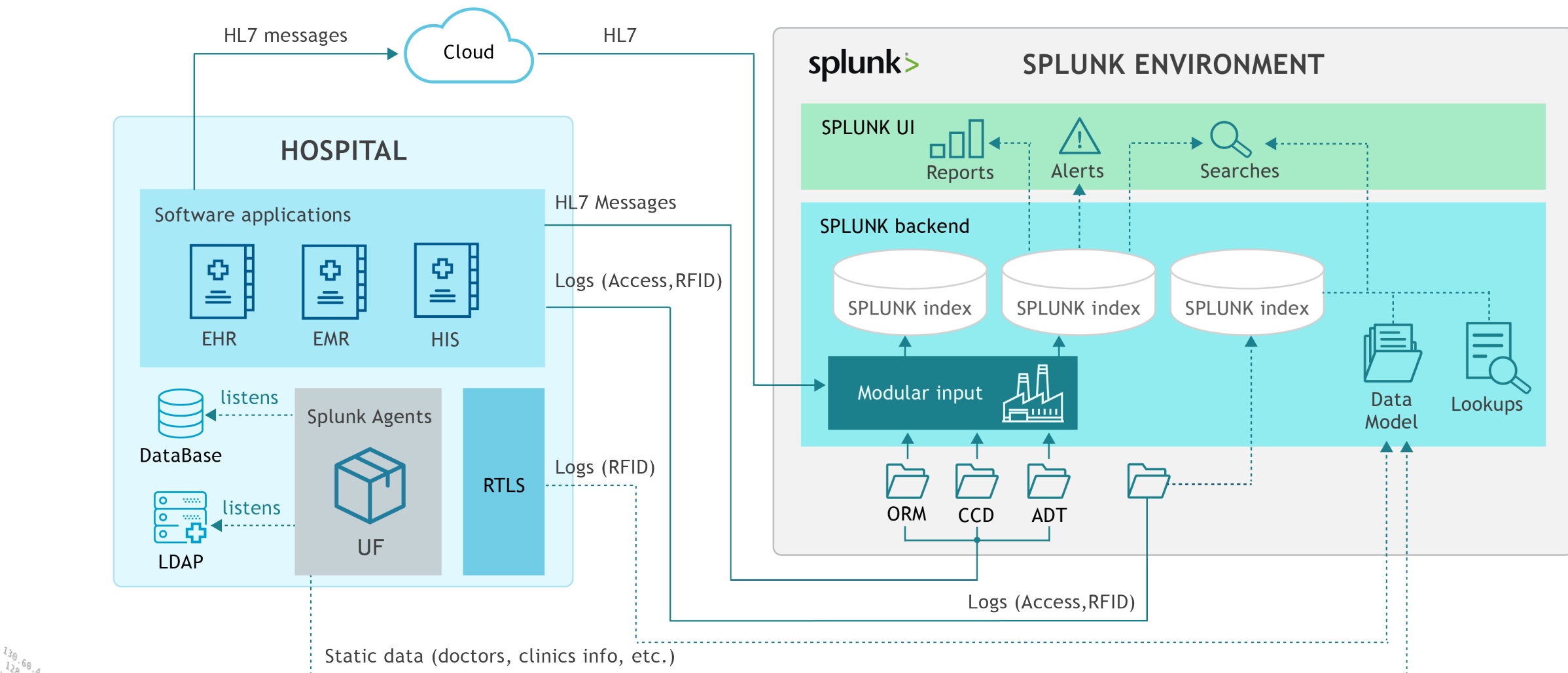


DATA SOURCES AND ARCHITECTURE

DATA SOURCES USED TO IDENTIFY CARETEAM



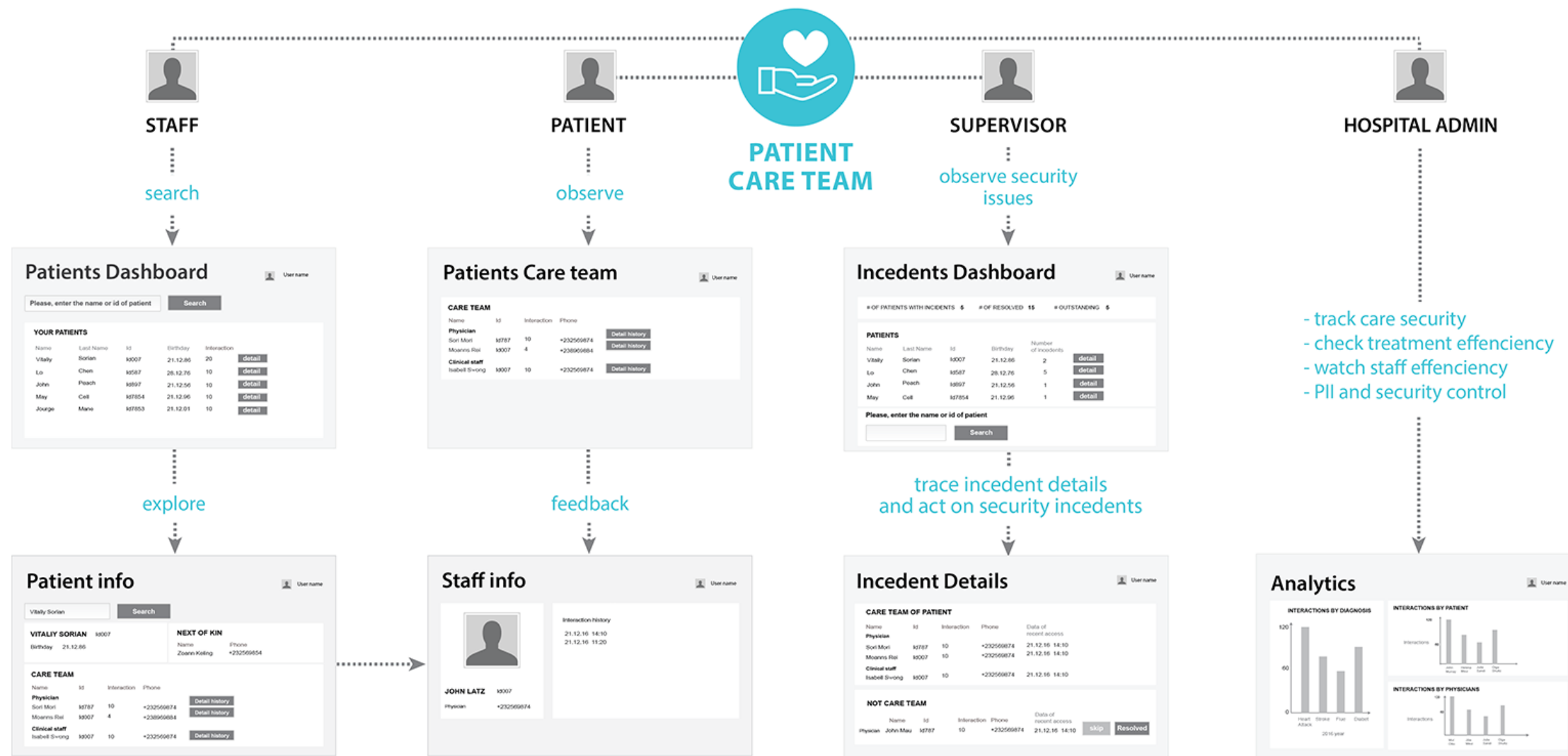
HIGH LEVEL ARCHITECTURE



A composite image featuring medical professionals. On the left, a male doctor in a white coat and stethoscope is shown in profile. On the right, a female doctor in a white coat is writing on a clipboard. The background is a teal gradient with a faint image of a group of people smiling. The text 'SOLUTION OVERVIEW' is centered in white.

SOLUTION OVERVIEW

APPLICATION SITEMAP

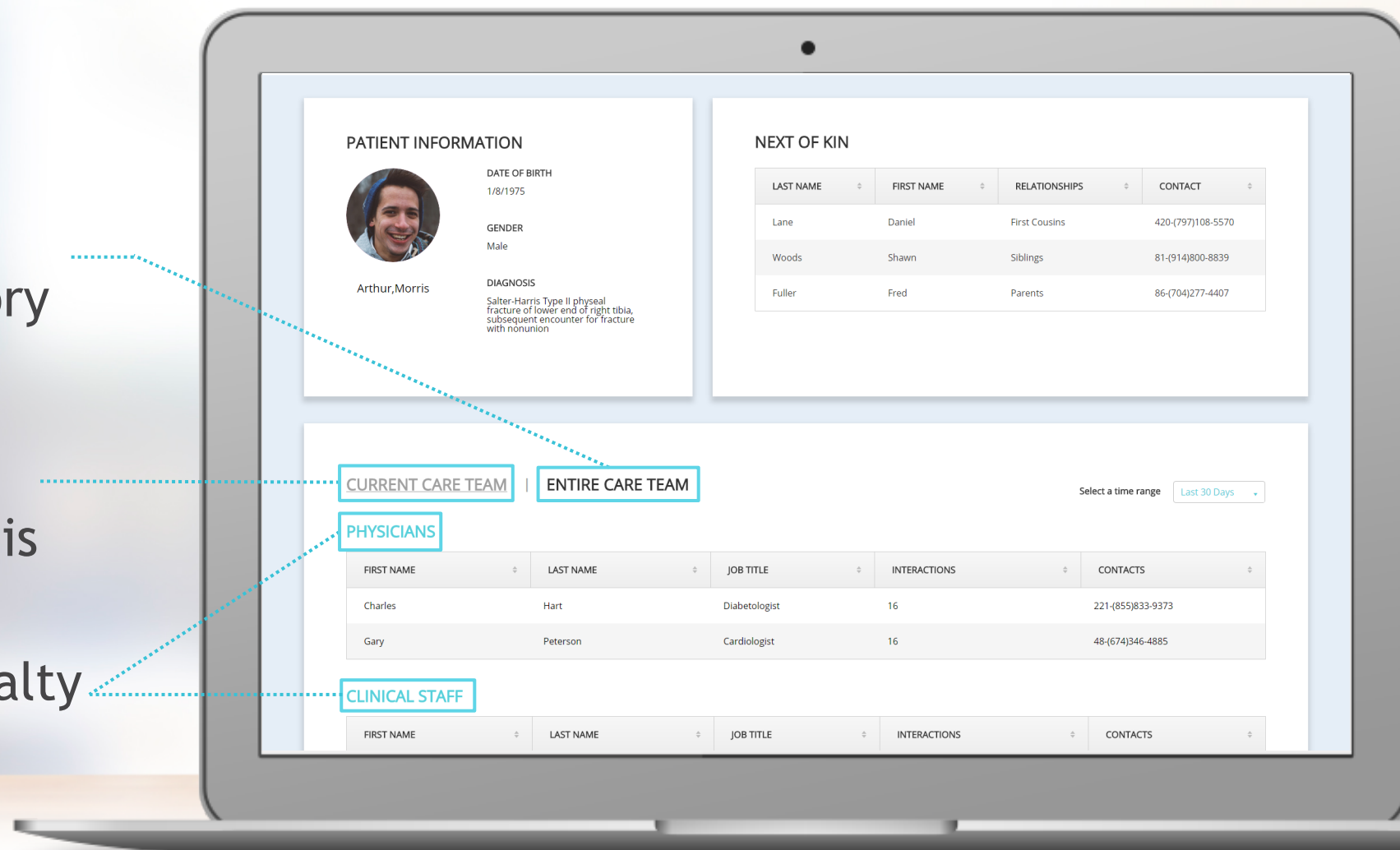


CARE TEAM IDENTIFICATION

Care team based on
full admissions history

Care team based on
most recent diagnosis

Breakdown by specialty

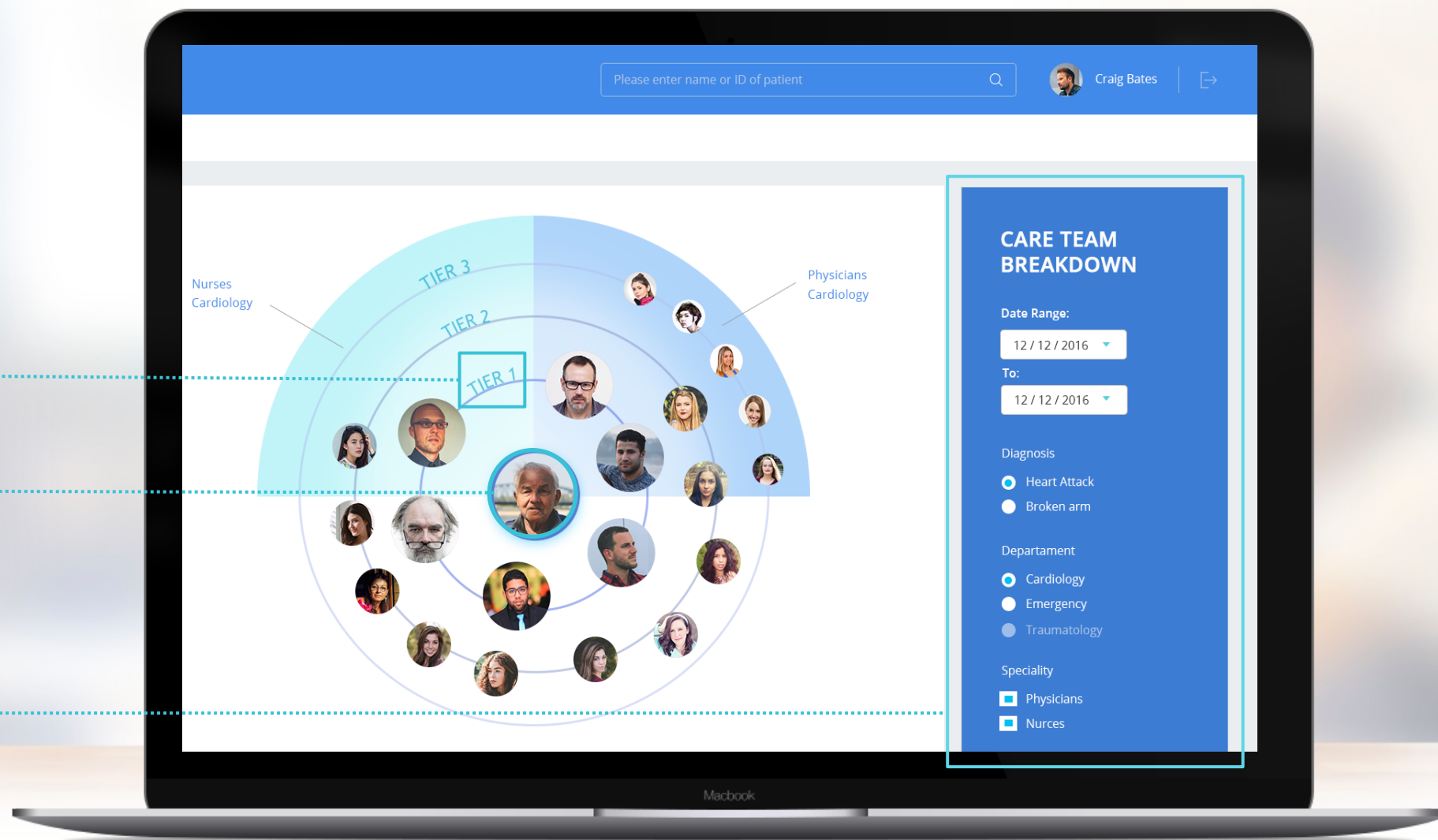


IDENTIFY KEY PERSONNEL

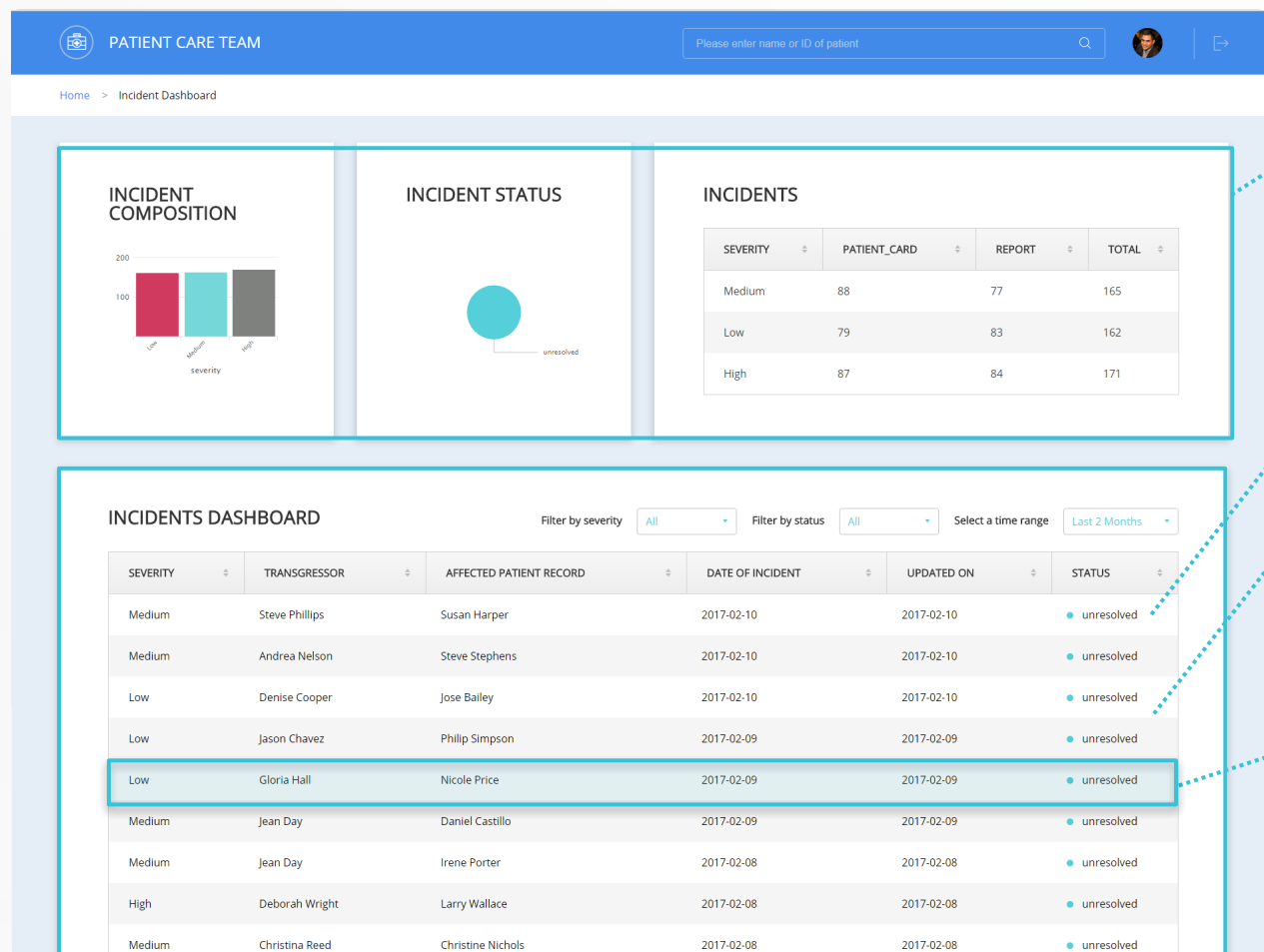
Key personnel
(tier-1)

Patient

Smart filtering



COMPLIANCE



Incidents summary & drilldown

Patient room access violation

Patient record access violation

INCIDENT DETAILS

INCIDENT ID 1486688280-DCTR0045

STATUS unresolved

TYPE report

EVENT TYPE edit

TIMESTAMP

APPLICATION ID
129

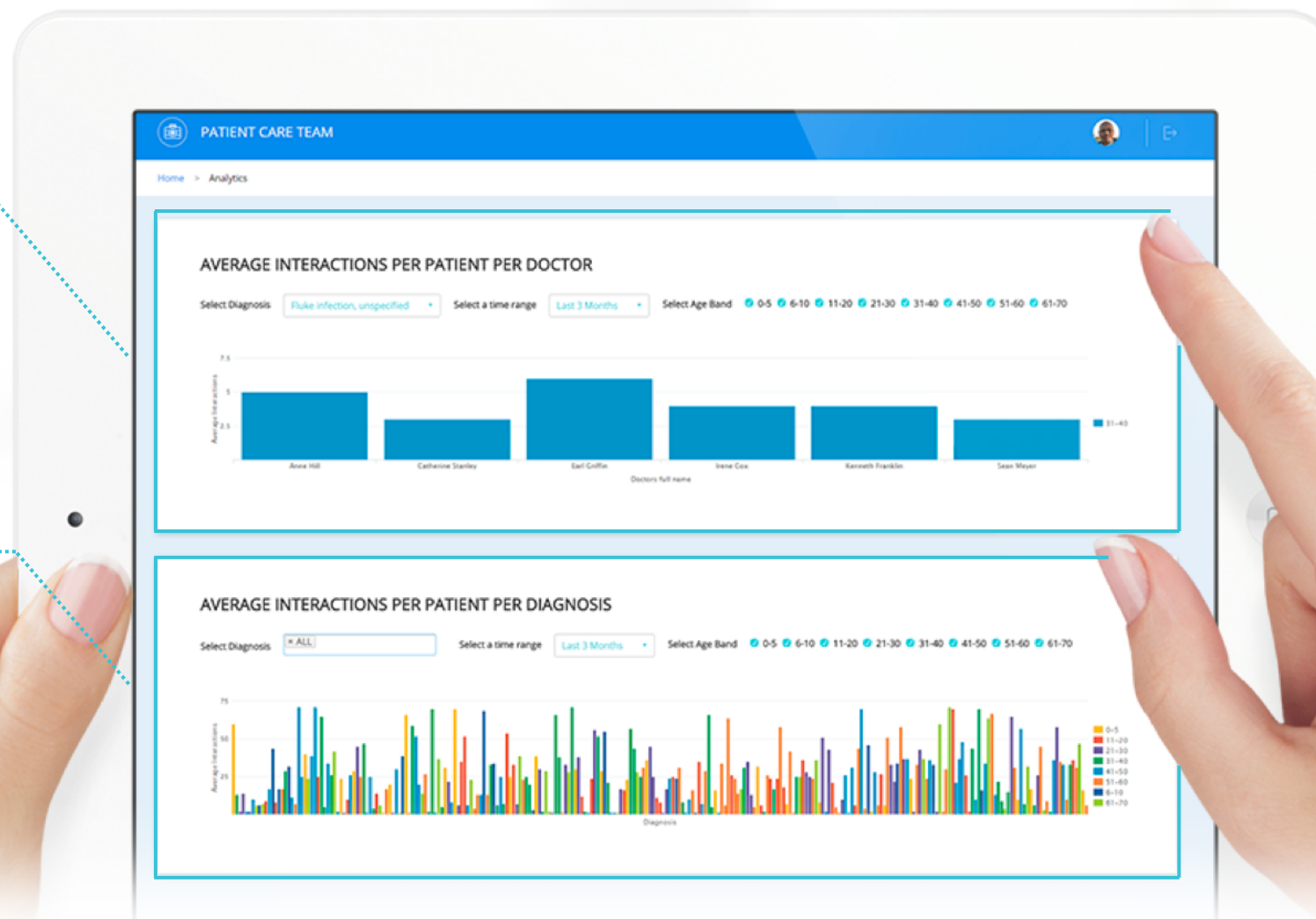
CLIENT IP
127.111.217.42

START PROGRESS

REPORTING

Interactions
report

Interactions insights
per diagnosis

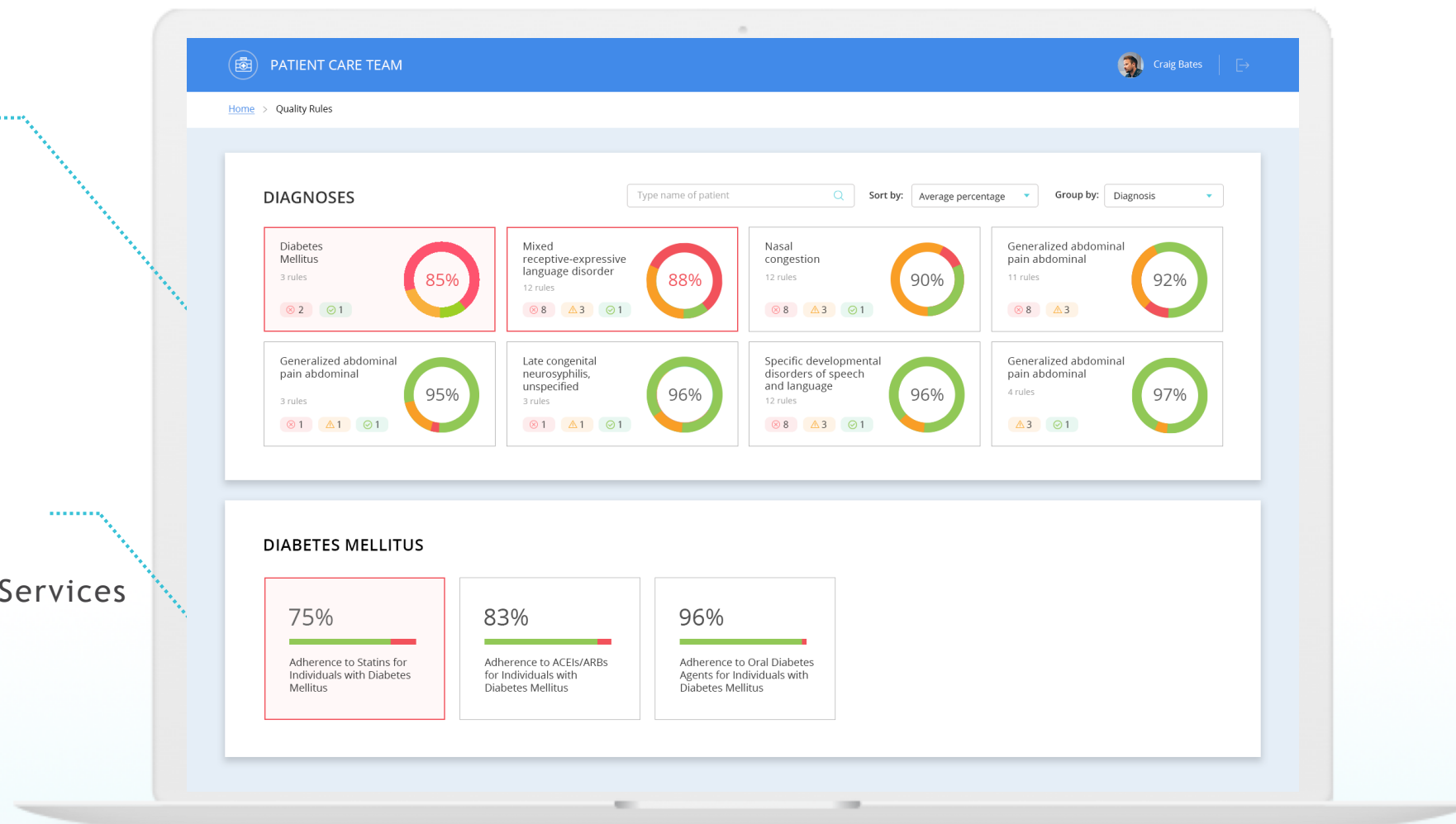


CARE GAP DETECTION

Care Gap Overview

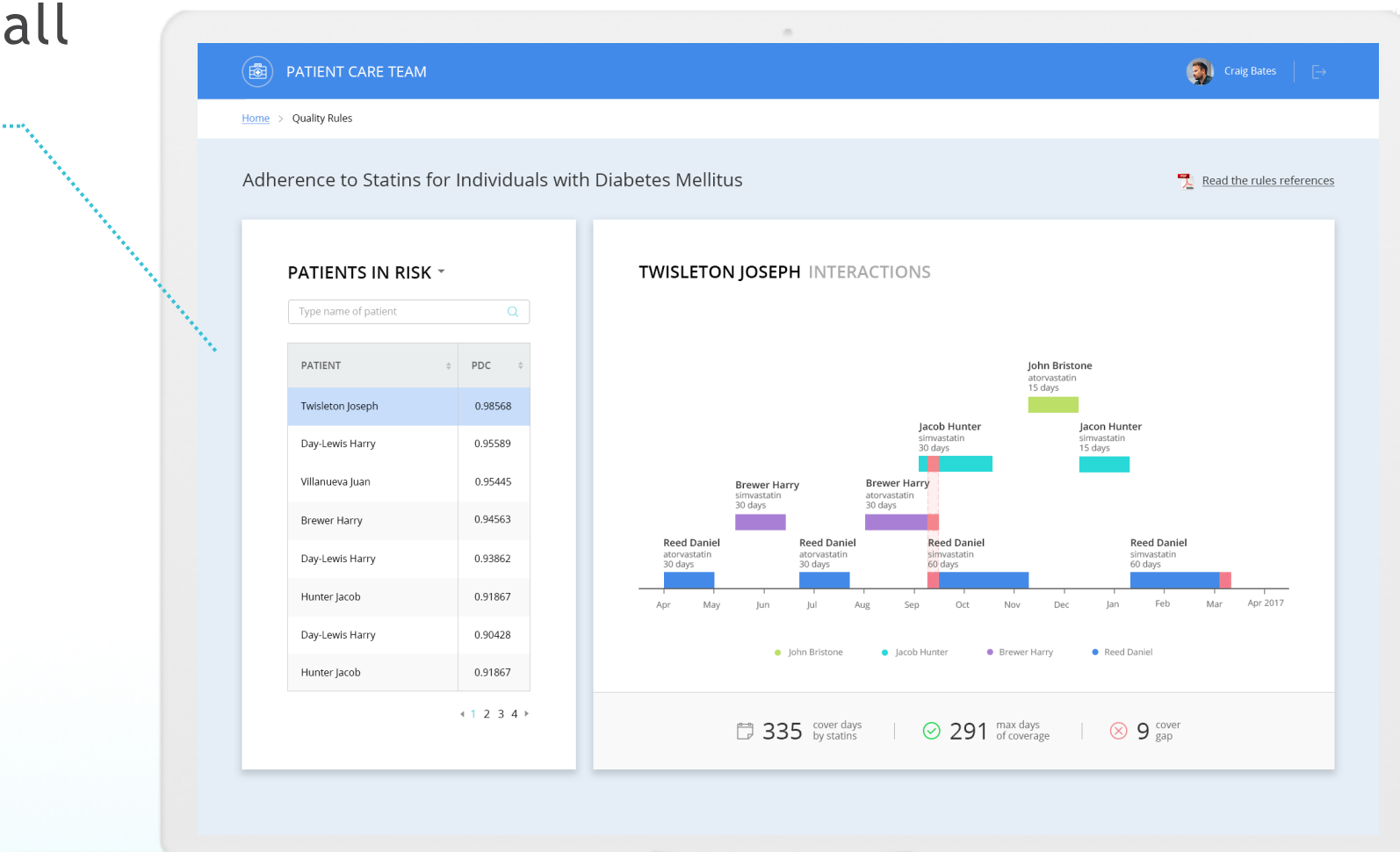
Care Quality Rules

<https://www.cms.gov>
Centers for Medicare & Medical Services

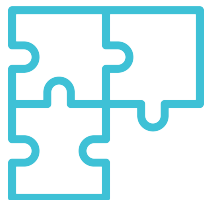


RULE LEVEL DETAILS

Patients at risk that fall under specific rule



POTENTIAL AND FUTURE ENHANCEMENTS



AREAS FOR FURTHER DEVELOPMENT AND IMPROVEMENTS

- Commercialization.
- Additional features (quality of service, care circles detection, cost effectiveness, extended and detailed fraud detection analytic).
- Visualization improvements (drilldowns and multi-dimensional searches).
- Robust model for all X12 transaction types. Processing and ad-hoc data processing



EPAM + SPLUNK COOPERATION FOOTPRINT

- Ability to deliver SPLUNK - based solutions from within EPAM labs.
- Help in testing, prototyping, verification of early versions of Splunk products.
- Ability to deliver EPAM vertical industry solutions based on Splunk products and EPAM domain knowledge.
- Collaborative knowledge and key assets will be shared with Splunk community.

LESSONS LEARNED



1. PERFORMANCE:

- Scheduled searches for alerts usually impact performance so separate search head for them worth consideration.
- Roles isolation (in our case patient/doctor) on Search head level was also very helpful and useful.
- Use Job inspector for queries profiling. (It's the basic one to detect performance problem)
- Tstats command was very useful along with “walklex” cli command for efficient queries optimization.
- Data Models should be used not only for further acceleration but even to keep your data in more structured way.

2. DEVELOPMENT:

- UI. It was very useful to first concentrate on development using simple/extended Splunk dashboards. UI customization should be done only after prototype is working.
- Use command line tools. Especially “btool”. It could take enormous amount of time to detect which config went wrong.
- Data “mutability” with KV store for storing user interactions was really neat.

LESSONS LEARNED



3. SPLUNK CAN BE USED:

- Splunk can be used much beyond its natural log aggregation and full-text search.

4. COST-EFFICIENCY:

- Always plan for expected data load.

5. HEALTHCARE SPECIFICS:

- PHI data masking for HIPAA compliance is supported out-of-the box
- Documents of HL7 v. 2.x can be successfully parsed and processed via Splunk Modular Inputs.



THANK YOU!

Patient Care Team The Journey

What did Splunk learn?

Getting Started

How did EPAM get started?

- ▶ Building Splunk Solutions ebook
 - <http://dev.splunk.com/view/dev-guide/SP-CAAEE2R>
- ▶ Dev.splunk.com for examples, tutorials
- ▶ New Quick Start
 - Guided “your first app” experience

BUILDING SPLUNK SOLUTIONS

Splunk Developer Guide

Grigori Melnik
Dominic Betts
David Foster
Liyang Jiang

splunk>

Foreword by Stephen Sorkin

Getting Started

New Quick Start bridges the gap

- ▶ <http://dev.splunk.com/view/quickstart>
- ▶ Guided “your first app sequence”
- ▶ Certification with Splunk Certified
- ▶ Best practices

Quick Start

Welcome to Quick Start: Developing your first Splunk app.

This Quick Start walks you through the process of creating an app using Splunk Web and explains how configuration files work together to create an app.

QUICK START

Quick start

Your First AppInspect

When developing an app, consider whether you want to have it [Splunk Certified](#). When Splunk certifies an app, other users know that the app meets Splunk's rigorous certification criteria. Your app will also be featured more prominently in search results.

QUICK START

Quick start

Before you begin

Create your first app

Add data

Report on data

Visualize data

Change navigation

Extras

Set \$SPLUNK_HOME

Your first AppInspect

Use macros to avoid index dependency

Use Macros To Avoid Index Dependency

In [Report on data](#) in this tutorial, the search you used in your dashboard referenced a specific index. However, as a recommended practice, you shouldn't include index definitions with your app. You could remove the specific index from your search, but then you'll have to include "index=*" in your searches instead. If your users want to restrict your app to searching in a specific index, they'll need to modify every search.

To work around this issue, you can use a macro that includes a default index to search, helping administrators to configure your app. For development, you can also set up a local version of the macro to reference your development index.

For more about macros, see [Use search macros in searches](#) in the *Knowledge Manager Manual*.

For a general description of using macros to avoid dependency on indexes, see [App Design Patterns - Creating Indexes](#) on Splunk Blogs.

Let's start out by creating a macro. In this macro, you'll specify an index that your app should look in for sendmail_syslog events.

1. In Splunk Web, click **Settings**, then click **Advanced search**.
2. Next to **Search macros** click **Add new**.
3. Under **Destination app** make sure your app is selected.
4. Under **Name** provide a name for your macro.
5. Under **Definition** enter:

```
index=hello_index
```

Your macro definition should look something like this:



QUICK START

Quick start

Before you begin

Create your first app

Add data

Report on data

Visualize data

Change navigation

Extras

Set \$SPLUNK_HOME

Your first AppInspect

Use macros to avoid index dependency

Test Data

How did EPAM test the Patient Care Team app?

- ▶ Started with Splunk EventGen
 - <https://github.com/splunk/eventgen>
- ▶ Built their own data generator for testing
- ▶ Saw bigger value with anonymized, real data
- ▶ SimData
 - Generate real-looking test data without samples
 - Here at Conf: “Fake Data for Real Apps”
 - Tuesday, 2:15 PM – 3:00 PM

Test Data

SimData

- Generate
- Demonstrate
- Create data

```

1 simulation webtraffic
2
3 entity WebServer(server_name) {
4     self.alive = true
5     self.capacity = 10.0
6     self.load = 0.0
7     self.ticks = 0
8     self.pages_served = 0
9     action serve_page(page_name, ip_address) {
10         page = one_of(Page[page_name=page_name])
11         self.pages_served = self.pages_served + 1
12         load_modifier = self.load + 1
13         response_time = page.service_duration * random(0.8, 1.2) * load_modifier
14         user = one_of(User[ip=ip_address])
15         tell user response(page_name)
16         timer {
17             name: "webserver.response_time.{{self.server_name}}.{{page_name}}"
18             value: response_time
19         }
20         log {
21             sourcetype: "weblog"
22             host: self.server_name

```

How did EPAM get data in?

- # Splunk Add-on Builder

- ▶ Getting data in should be easy
- ▶ Getting your app certified should be easy
- ▶ Here at Conf: “: “From API to Easy Street Within Minutes Using Add-on Builder”
 - Wednesday, 1:10 PM-1:55 PM

Getting Data In

Splunk Add-on Builder

► <http://>

► Build

• Mod

• Ale

• Fie

• CIP

• Ad

► Valid

Hello World! | **Validate & Package** | Manage Source Types | Extract Fields | Map to Data Models | Create Alert Actions

Validate & Package

Click **Validate** to validate your add-on against best practices and other rules, and to determine whether your app is ready for Splunk App Certification. When you have finished creating your add-on, click **Download Package** to create and download the SPL package file. [Learn more](#)

Overall Health Report

100

Ready for certification

Congratulations, your add-on is ready to submit to Splunk App Certification.

Category	Score	Status
Error	0	0
Warning	0	0
Pass	86	86

Validation Results

Thank You

Don't forget to **rate this session** in the
.conf2017 mobile app

splunk> .conf2017