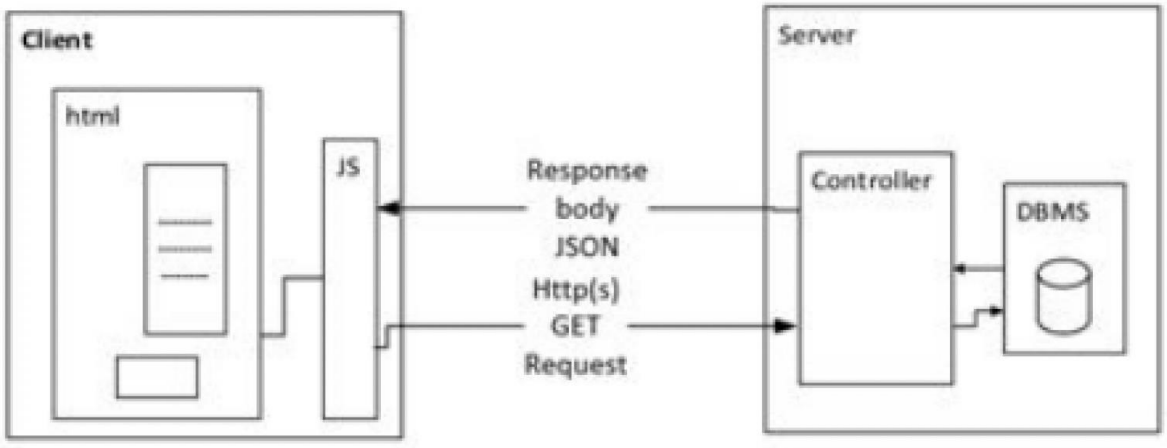
Fragensammlung zur Matura (extramural)

1) Beschreibe die Architektur unseres APIS?



a) Server Client Architektur

Bei unserem Beispiel wird die REST-Schnitte miteinbezogen. (REST steht für Representational State Transfer)

b) Beschreibung

Die Server-Client-Architektur besteht aus zwei wesentlichen Komponenten: Dem Client (beispielsweise ein Laptop öffnet unsere Webseite mittels einem Internet-Explorer), sowie dem Server, welcher für die Datenverarbeitung zuständig ist.

Server

Der Server besteht in diesem Fall aus einem Controller, sowie einem sogenannten Datenbankmanagementsystem (kurz DBMS). Diese arbeiten “Hand in Hand”. Der Controller ist für die “präsentation” oder anders gesagt für die Übergabe und Aufbereitung der Datensätze zuständig. Das DBMS kümmert sich um das Bereitstellen der Datensäze.

Client

Der Client bzw. die Client-Ansicht wird in diesem Fall mittels einem Internet-Browser m glich gemacht. Dieser verarbeitet HTML- sowie JavaScript-Code in Kombination. Der JavaScript-Code ist für die Aktionen bzw. Funktionen im Browser zuständig, nachdem HTML-Code nur die Präsentation der Inhalte durchführt. Die Inhalte des HTML-Codes werden mittels JSON-Dateien übergeben, nachdem das regelmäßige Senden des gesamten Codes zu aufwendig wäre. Rückmeldungen bzw. Rückgabewerte des Clients werden mittels HTTP(s)-GET-Requests übergeben. Diese werden mittels dem JavaScript-Code generiert.

Die HTML-Dateien, welche im Client präsentiert werden, werden mittels TypeScript bzw. Angular generiert.

c) Wir haben einen Server und einen Client (Angular)
d) Server:
   i) Module, Repository, TOM-Cat, SpringBoot, JPA, Datenbank, Tests, Controller
e) Client:
   i) Angular, Routing, Services (ts), Components (html, ts), Typescript wird zu Java umgewandelt, HTML, CSS

Genauere Erklärung zu DOM:

Document Object Model (DOM, engl. für Dokumenten-Objekt-Modell)

- ist eine Spezifikation einer Programmierschnittstelle, welche HTML oder XML-Dokumente als eine Baumstruktur darstellt, in der jeder Knoten ein Objekt ist, welches einen Teil des Dokumentes repräsentiert, z. B. einen Absatz, eine Überschrift, ein Video oder etwa eine Tabellenzelle. Die Schnittstelle ist plattform- und programmiersprachenunabhängig und erlaubt damit standardisiert, die Struktur und das Layout eines Dokumentes zu verändern.
- Im Webbrowser bildet dies einen wichtigen Baustein für dynamische Webseiten.
- In unserem Fall manipulieren wir mittels TypeScript den DOM, damit wir Inhalte im HTML-Code präsentieren können. Ein wesentlicher Anwendungsfall ist das Erstellen der Listen mittels TypeScript. Dadurch wird in den bereits geschriebenen HTML-Code eingegriffen, um die einzelnen Einträge zu erstellen.

HTTP-Protokolle:

Im HTTP(s)-Protokoll ((sicheres) Hypertext Transfer Protocol) gibt es verschiedene Anfragemethoden (englisch: request methods), die es dem Browser ermöglichen, Informationen, Formulare oder Dateien an den Server zu senden.

Wahl der Anfragemethode

Die Wahl der Übertragungsmethode hängt, will man es richtig machen, nicht etwa von der Präferenz des Programmierers ab, sondern folgt eigentlich ganz einfachen Regeln:

I. Werden durch den Request lediglich andere Daten als Antwort empfangen, so ist die GET -Methode die richtige Wahl.
II. Werden durch den Request Daten auf dem Server verändert, ist die [POST] -Methode die richtige Wahl.
III. Werden Daten für Logins, insbesondere Passwörter übermittelt, dann ist nur POST die einzig richtige Wahl.

GET

Mit der GET -Methode können Sie eine Ressource (zum Beispiel eine Datei) vom Server anfordern. Dabei wird ein Parameter (z. B. übertragene Formulardaten), getrennt durch ein Fragezeichen, zum URI hinzugefügt.

POST

Mit der POST -Methode k nnen Sie gro e Datenmengen (wie Bilder oder HTML-Formular -Daten) zur weiteren Verarbeitung zum Server senden.

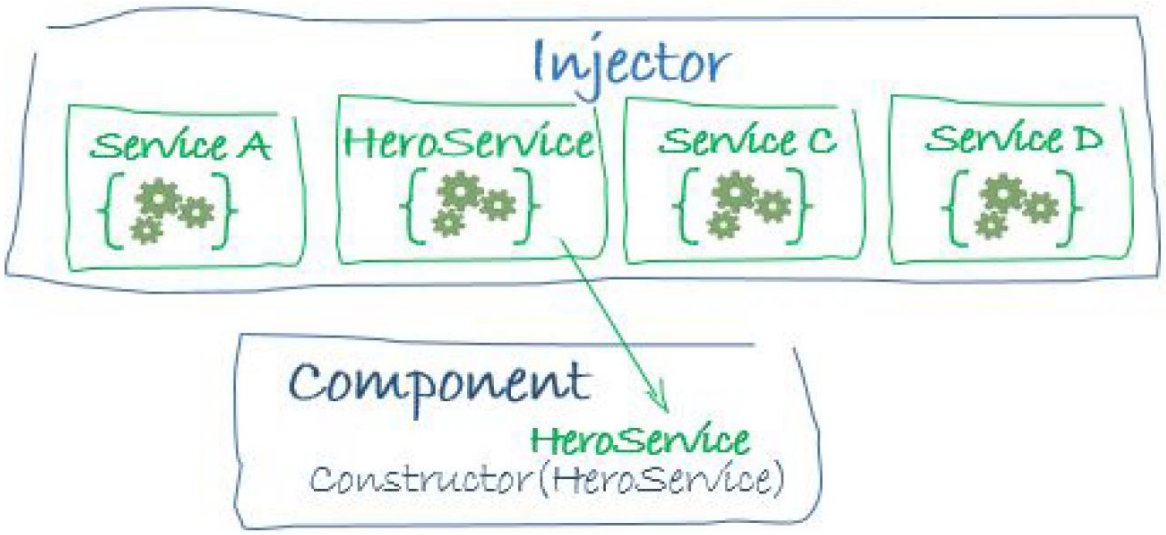
2) Liste die Technologien auf, die am Server zum Einsatz kommen. Beschreibe jeweils aus welchen Komponenten diese jeweils aufgebaut sind.

- **Tomcat:** ist ein Open Source Webserver, auf dem in der Sprache Java geschriebene Web-Anwendungen ausgeführt werden.
- **POM-Datei:** Das ist eine Konfigurationsdatei für Maven Projekte oder auch "Bauanleitung für die Applikation". Speichert die Informationen eines Softwareprojekts werden, in XML-Format. Es bietet eine einfache Möglichkeit, um weitere Libraries in die eigene Applikation einzubinden. Datei: pom.xml
- **JPA:** JPA ist ein Standard , steht für Java Persistance API und ermöglicht das Speichern von Java Objekten in die Datenbank. Ohne JPA müssten wir etliche SQL Statements schreiben, um unser Objektmodell (Java) in das relationale Modell (Datenbank) abbilden zu können. JPA ist dabei eine Open Source Spezifikation und wird z.B. von Hibernate, Eclipselink, Toplink, Spring Data JPA implementiert. Wir benutzen es als Annotations (@).Starten wir die Applikation werden abhängig von den Einstellungen in application.properties (create) die Tabellen in der Datenbank neu erstellt.
- **Hibernate:** Ist ein Open-Source ORM-Framework für Java . Hibernates Hauptaufgabe ist die objektrelationale Abbildung . Dies ermöglicht es, gewöhnliche Objekte mit Attributen und Methoden in relationalen Datenbanken zu speichern und aus entsprechenden Datensätzen wiederum Objekte zu erzeugen. Beziehungen zwischen Objekten werden auf entsprechende Datenbank-Relationen abgebildet. → implementiert JPA → Datenbankanbindung ohne "richtigen" SQL-Code.
- **Spring Boot:** Spring Boot ist ein Framework für Java-Plattformen und wird genutzt, um RESTful Webservices zu erstellen. Damit können wir ebenfalls mit mobilen Clients auf das Service zugreifen oder von einer Webseite, um dynamische Inhalte zu laden. Es ermöglicht uns eigenständige Spring Applikationen zu erstellen → .jar Datei, die direkt ausgeführt werden kann. Der Webserver muss nicht extra gestartet und die Applikation darauf deployed werden, Spring Tomcat eingebettet hat und beim Starten der Applikation gleich ausführt. Es besitzt eine Voreingestellte POM Datei, um die Maven Konfiguration zu erleichtern.
- **Datenbank:** Ist der Speicherort für alle Daten. Der Server kommuniziert über JPA mit der Datenbank. Die Datenbank sollte sich in einem separaten abgesicherten Netzwerk befinden, damit die Daten nicht gestohlen/manipuliert/gel scht werden k nnen. Des weiteren sollten Brute Force Attacken mit einem Sicheren Passwort gesichert werden. Das Passwort befindet sich in unserem Projekt unter application.properties. Wie bereits erwähnt wird auf die Datenbank nicht direkt vom Client zugegriffen, dazwischen befindet sich die Business- oder Application Logic, welche die benötigten Daten liefert. → Client schickt Request → Business Logic (Controller) verarbeitet es → greift bei Bedarf (meistens der Fall) auf die Datenbank zu → verarbeitet Daten → Daten an den Client mittels Service als JSON.
- **Modelklasse:** (Persistenzschicht) Aus den Modellklassen wird mit Hilfe der JPA-Annotationen ein passendes Datenbankschema erstellt (muss es aber nicht, falls eine alte Datenbank existiert, welche nicht dem FHIR-Standard entspricht). Die Model Klassen ermöglichen es uns, das Laden und Speichern von den Objekten in die Datenbank, leicht umzusetzen. Man spricht von "Objekten persistieren". Ohne JPA müssten wir die Java Klassen und die Datenbank erstellen. Dabei ist es sehr wichtig auf die Annotationen der Relationen und der Vererbungshierarchie zu achten.
- **Repository:** (Persistenzschicht) Diese Komponente greift auf die Datenbank zu. Wir benötigen für jede Modellklasse, mit denen der Client interagiert (z.B. Patient), ein Repository. Es erstellt automatisch die CRUD (Create, Read, Update, Delete) Befehle

für die Datenbank. Die Repositorys ermöglichen uns ohne SQL-Skripts zu codieren und verhindert somit SQL-Injections.

- **Test :** (Test der Persistenzschicht) Um die korrekte Implementierung unsere Persistenzschicht (Repositorys & Modellklassen) zu testen verwenden wir automatisierte Tests. Es wird ein Objekt erstellt und über die Repositories in der Datenbank gespeichert. Der Gespeicherte Inhalt wird geladen und mit dem Originalobjekt verglichen. Wenn beide gleich sind, passt alles.
- **Converter :** Konvertiert die von der Datenbank erhaltenen Daten, dass sie sie dem FHIR Standard entsprechen. Beispiel Set<String>: um nicht extra eine Tabelle mit Strings auf der Datenbank zu erstellen, werden diese in einem “string” Feld gespeichert. Beim Aufrufen von der Datenbank wird der String in ein Set<String> konvertiert.
- **Controller :** Dies ist die Schnittstelle zur Außenwelt (Clients) unserer Applikation. Diest ist unsere REST Schnittstelle zu unserem Client. Er verarbeitet die Requests des Clients. Spring Boot bietet hierfür Controller (MVC, Model View Controller) an. Ein Controller verarbeitet HTTP Anfragen wie Get, Post, Put, Delete. Über das Repository greift es auf die Datenbank zu, verarbeitet die Daten und schickt die verarbeiteten Daten als JSON an den Client.

3) Liste die Technologien auf, die am Client zum Einsatz kommen. Beschreibe jeweils aus welchen Komponenten diese jeweils aufgebaut sind.
   a) Framework: Als Basis des Clients dient das Framework Angular, welches mit Typescript entwickelt und zu JavaScript umgewandelt wird. Darüber hinaus wird reguläres HTML, mit zusätzlichen angular spezifischen Tags und Parametern, und CSS genutzt, wobei wir überwiegend Bootstrap als CSS-Framework verwenden.
   b) Komponenten:
      i) Services: durch Dependency Injection wird den Komponenten der Service "injiziert". Der große Vorteil ist dabei eine geordnete Struktur des Codes zu erreichen ohne "doppelten Code". Ein einziger Service kann von mehreren Komponenten übernommen werden.



Beispiel: Dataservice enthaltet Methoden zur Datenmanipulation (createPatient, updatePatient), welche durch eine Instanz dieses "Services" im Konstruktor übergeben wird.

      ii) Routing: Es ist üblich das Routing durch eine separate Module Klasse zu erzeugen. app-routing.module.ts. Wenn etwas angeklickt wird oder eine URL eingegeben wird, kommt es beim APIS über Routing an die lokale Komponente. Der GET Request wird dabei zuerst lokal abgefangen und bearbeitet. Der Server wird erst angesprochen, falls lokal kein Pfad vorhanden ist. Die Seite kann aktualisiert werden, ohne den Server zu kontaktieren.
      Ein typischer Route hat zwei Eigenschaften:
      I path: Eine Zeichenfolge, die mit der URL in der Adressleiste des Browsers überstimmt.
      II component: Die Komponente, die der Router beim Navigieren zu dieser Route erstellen soll.

      Routen teilen dem Router mit, welche Ansicht angezeigt werden soll, wenn ein Benutzer auf einen Link klickt oder eine URL in die Adressleiste des Browsers einfügt. Durch importieren der Komponenten gibt man einen Ort an auf die der Router zugreifen soll.

      I: Eine URL wird in die Adressbar eingegeben → Passende Seite wird aufgerufen
      II: Links werden angeklickt → Navigation zur Seite
      III: Back & Forward Buttons werden unterstützt

iii) Model: FHIR-Standard (JSON) wird gespiegelt. Der Client bekommt nur die REST Schnittstelle vom Server mit. Die Datenbankstruktur ist nicht relevant für den Client.

Beispiel:

```
export class PatientModel {
    constructor(
        public name : [ HumanName ], // A name
associated with the patient
    ) {}
}

export class HumanName{
  [x: string]: any;
    public id: string = ''
        public use: string = ''
        public text: string = ''
        public family: string = ''
    constructor(
        id: string = '',
        use: string = '',
        text: string = '',
        family: string = ''
    ){this.id=id;this.use=use;this.family=family,
this.text=text}
}
```

Der Patient hat ein Attribut “name” mit dem Datentypen HumanName, welcher gleich aufgebaut ist wie am Server.

iv) NgModules: Auch als Funktion Module bekannt.
NgModule-Metadaten:

I. Gib an, welche Komponenten, Anweisungen und Pipes zum Modul gehören.
II. Macht einige dieser Komponenten, Anweisungen und Pipes öffentlich, damit die Komponenten Template anderer Module sie verwenden können.
III. Importiert andere Module mit den Komponenten, Anweisungen und Pipes, die Komponenten im aktuellen Modul benötigt werden.
IV. Bietet Dienste, die die anderen Anwendungskomponenten verwenden können.

Jede Angular App verfügt über mindestens ein Modul, das Root-Modul. Sie booten dieses Modul, um die Anwendung zu starten.

Das Root-Modul ist alles, was Sie in einer einfachen Anwendung mit wenigen Komponenten benötigen. Wenn die App wächst, überarbeitet sie das Root-Modul in Feature-Module, die Sammlungen verwandter Funktionen darstellen. Anschließend importieren sie diese Module in das Root-Modul.

v) Direktives: verbindet Applikationsdaten mit dem DOM. Wir verwenden die NgFor-Direktive, um ein Array von Elementen zu durchlaufen und mehrere Elemente dynamisch zu erstellen aus einem template Element.

Das Template ist das Element, an der die Direktive angehängt ist.
Wir können mehrere NgFor-Direktiven zusammenschachteln.
Wir können die Index des Elements abrufen, über das wir eine Schleife durchführen, indem wir einer Variable im NgFor einem Index zuweisen.

vi) Pipes: Ausgabe der Outputs im speziellen Format. Beispiel: Datumsformat. JavaScript Daten werden passend formatiert für die HTML.

4) Zähle auf und beschreibe, welche Protokolle verwendet werden, um Daten zwischen dem Server und dem Client zu übertragen.
   a) TCP/IP (Transmission Control Protocol/ Internet Protocol)
   b) HTTPS/HTTP

HTTP Method	CRUD	Entire Collection (e.g./users)	Specific Item (e.g. / users/123)
POST	Creat	201(Created), 'Location' header with link to /users/{id} containing new ID.	Avoid using POST on single resource
Get	Read	200 (OK), list of users. Use pagination, sorting and filtering to navigate big lists.	200 (OK), single user. 404 (Not Found), if ID not found or invalid.
PUT	Update/Replace	405 (Method not allowed), unless you want to update every resource in the entire collection of resource.	200 (OK) or 204 (No Content). Use 404 (Not Found), if ID not found or invalid.
Patch	Partial Update/ Modify	405 (Method not allowed), unless you want to modify the collection itself.	200 (OK) or 204 (No Content). Use 404 (Not Found), if ID not found or invalid.
DELETE	Delete	405 (Method not allowed), unless you want to delete the whole collection — use with caution.	200 (OK). 404 (Not Found), if ID not found or invalid.

RESTful HTTP(s)-Verben aus https://restfulapi.net/http-methods/

- CRUD ist ein Akronym für die vier fundamentalen Operationen des Datenmanagement :
  - Create (POST): Neue Daten erstellen
  - Read (GET): Bestehende Daten selektieren und zur weiteren Verarbeitung bereit stellen
  - Update (PUT): Bestehende Daten aktualisieren
  - Delete (DELETE): Veraltete Daten löschen
- Oftmals handelt es sich bei der grafischen Benutzeroberfläche eines CRUD-Frameworks um ein simples HTML-Interface. Typischerweise berücksichtigt das CRUD-Framework einzelne Transaktionsschritte . Dies hat zur Folge, dass Daten nur gespeichert werden, wenn innerhalb der HTML-Oberfläche der Speichern- bzw. Weiter-Button gedrückt wurde. Ist dies der Fall, so wird die Update-Operation ausgeführt.
- Das CRUD-Framework weist selbstverständlich ein äquivalentes Verhalten für die verbleibenden CRUD-Operationen auf. Es handelt sich bei einer CRUD-Operation folglich um einen atomaren Vorgang.

- Atomare Operationen sind in diesem Zusammenhang von Interesse, da moderne Software -Anwendungen oftmals als Mehrbenutzersystem realisiert werden. Ein CRUD-Framework erlaubt Lesen und Schreiben eines Datensatzes auch dann, wenn beide Operationen zeitlich stark versetzt erfolgen. Trotzdem ist es anderen Personen gestattet, während dieser Zeit denselben Datensatz auszulesen. Folglich wurde der Datensatz nicht gesperrt.

5) Beschreibe den Ablauf der Übertragung der Daten zwischen Client und Server.
   a) Kurze Antwort: Server: Controller, Client: DataService
   b) Lange Antwort:
   c) Am Client wird auch eine Aktion (z.B. Klick von User) in Request an den Server geschickt. http-Request = im Header http-Verb mit Parameter.
   d) Server hat in unserem Fall den Controller
   e) Parameter im http-header bestimmen, welcher Controller die Request bearbeitet (z.B.: Ein Put für Patient mit der Id 4 bearbeitetet der PatientController)
   f) Der Controller „liest" den Request und übersetzt ihn für das Repository
   g) Das Repository greift auf die Datenbank zu und führt den vom Controller erhaltenen Befehl aus
   h) Danach liefert das Repository dem Controller die Daten aus der Datenbank
   i) Der Controller nimmt die erhaltenen Daten und formt sie zu einem http-Response um
   j) Die vom Controller erstellte http-Response (mit JSON im Body) wird an den Client geschickt
   k) Das DataService im Client empfängt diese Response
   l) Je nach vorangehenden Befehl wird der erhaltene Datensatz behandelt.
   m) Request geht nach einem Klick auf ein Objekt in den Server ein. Controller verarbeitet den Request.
   n) Repository holt die Daten aus DB und formuliert HTTP Response(JSON im Body)
   o) HTTP Response geht beim Client in den Data Service ein und die Daten werden angezeigt (Je nachdem was der Benutzer geklickt hat.)

- Der Client schickt eine Request an den Server. Adressiert wird diese durch einen Link mit Parametern damit der Server die Anfrage an den richtigen Controller leiten kann (z.B. phc.at/user/u-01). Die Request selbst kann noch zusätzlich Daten im Request-Body beinhalten und hat diverse Parameter im Request-Header (z.B. Methode, CORS, …)
- Die Anfrage wird über http/https zum Server geleitet.
- Nun sucht der Server anhand der Parameter in der URL und der Methode im Request-Header (GET, PUT, POST, DELETE) den richtigen Controller und führt diesen aus. Dabei werden in unserem Fall immer Daten über das Repository in der Datenbank abgerufen, eingefügt verändert oder gelöscht. Sollte der Controller oder sogar der Server nicht existieren, wird ein „404 Not Found"-Error zurückgeschickt.
- Wurde die Methode/Funktion hinter dem Controller ausgeführt, werden die daraus resultierenden Daten als Response zurück an den Client gesendet. Diese werden vom Dataservice empfangen und abhängig vom Auslöser verwendet.

Zähle zwei Beispiele für einen sinnvollen Einsatz von FHIR auf. Wo wird dabei FHIR eingesetzt?
Grundsätzlich ist FHIR für den medizinischen Bereich vorgesehen. Im Folgenden beziehen sich alle Beispiele auf diesen Bereich:
Spezifische Produkte:

- Apple – Mobile Healthcare Applikationen: Apple nutzt für die Kommunikation zwischen z.B. der Applewatch und IPhone FHIR bei der Übertragung der gesammelten medizinischen Daten. Auch können diese Daten an externe „Services" in FHIR-Struktur weitergeschickt werden.
    - KIS – Krankenhausinformationssystem: Es ist sinnvoll alle Strukturen, vom Repository, bis hin zur Kommunikation zwischen Geräten auf FHIR zu setzen.
- Allgemeine Anwendungsbereiche
    - Einrichtungs-interne Interoperabilität
    - Einrichtungsübergreifende Kommunikation
    - Abrechnungsrelevante Daten für die Krankenkasse
    - Regionale und nationale Netzwerke z.B.: ELGA, KIS, RIS
    - Mobile Applikationen

6) Welche Komponenten sind am Server und am Client für den Datenaustausch zuständig? Beschreibe jeweils die Funktionalität der Komponente.
   a) Client: DataService
      i) Im DataService wird die URL der jeweiligen Ressource angegeben, wo dann ein http-Request mit http-Verb an den Server geschickt werden kann
   b) Server: Controller
      i) Der Controller empfängt/bearbeitet die Reuests vom Client und schickt sie ggf. über das Repository an die Datenbank weiter.
      ii) Im Controller wird ein JSON erstellt welches über ein http-Response an den Client (Java Script) geschickt wird. Die Kommunikation zwischen Client und Server verläuft asynchron. Dies bedeutet, dass ohne Blockieren des Prozesses durch bspw. Warten auf die Antwort des Empfängers (wie bei synchroner Kommunikation der Fall) der Austausch stattfindet.

7) Welche Datenformate werden zwischen Client und Server ausgetauscht? Beschreibe examplarisch den Aufbau eines der Dateneinheiten.
   a) Kommunikation läuft über Http(s)
      i) Client sendet den Request (Create, Read, Update oder Delete)
      ii) Server antwortet mit http Response mit JSON, XML oder nur HTML im Body
   b) Aufbau Request
      i) Header: CRUD operation, Absender, Format etc., http version
      ii) Body: Zusatzinformationen optional z.B. bei einem Post Befehl die abzudatenden Daten (im JSON oder XML Format)
   c) Aufbau Response
      i) Header: HTTP Status, http version …
      ii) Body: JSON, XML Daten im Body
   d) Quelle: https://developer.mozilla.org/en-US/docs/Web/HTTP/Messages

8) Welche http Endpoints gibt es am Server? Liste diese mit den notwendigen Kriterien tabellarisch auf.
   a) Was sind Endpoints?

      Ein Endpunkt ist das Ende eines Kommunikationskanals. Wenn eine API mit einem anderen System interagiert, gelten die Berührungspunkte dieser Kommunikation als Endpunkte. Oft erfolgt der Zugriff über eine URL, an welche HTTP-Anforderungen gesendet werden und eine Antwort erwartet wird. Endpunkte geben an, wo Ressourcen liegen, auf die andere Systeme zugreifen können.

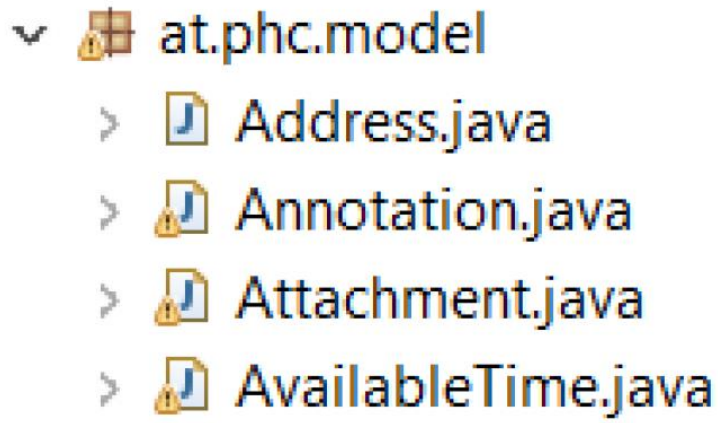
      Bei unserem Server:

URL	POST	GET
/api/<Resource>/	Einen Datensatz einer Ressource hinzufügen	Alle Datensätze der Resource auslesen oder mit Angabe der ID der Resource: /id -> Einen bestimmten Datensatz der Resource auslesen

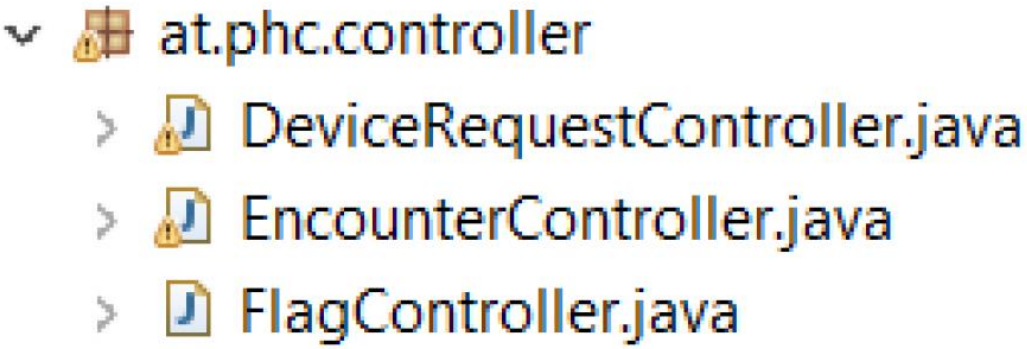
PUT	DELETE
Einen Datensatz einer Ressource aktualisieren/updaten (mit Angabe der ID -> /id)	Einen Datensatz einer Ressource löschen (mit Angabe der ID -> /id)

- /api/patient
- /api/bodystructure
- /api/encounter
- /api/observation
- /api/practitioner

9) Beschreibe den Zusammenhang zwischen dem MVC Konzept und den verwendeten Komponenten am Server. Was würde dem M, was dem V und was dem C entsprechen?
   a) M Das MVC-Konzept besteht aus den Komponenten Modell, View und den Controllern.
   b) Modell:



c) Das Modell auf unserem Server sind die erstellten Klassen mit den Attributen. Zusammen mit den Annotations ergibt sich ein Modell-Netz, welches auch in einer Datenbank abgebildet werden kann
d) View:
e) Das View ist die Form, in der die Daten an den Client geschickt werden, also das JSON-Format
f) Controller:



g) Die Controller regeln, wie die Clients auf die Daten zugreifen können

10) Beschreibe die Aufgabe von FHIR im medizinischen Umfeld.
    a) Das Gesundheitswesen basiert auf Kommunikation und Datenaustausch zwischen den verschiedenen Gesundheitsdienste-Anbietern. Damit diese Kommunikation funktioniert und keine Komplikationen aufweist, braucht man Kommunikationsstandards.
    b) FHIR ist ein Standard von HL7 und definiert eine Datenstruktur siehe Frage 7, die bei der Implementierung von Software eingehalten werden muss. Dieser Standard ermöglicht es, medizinische Daten und Abläufe, trotz unterschiedlicher Systeme einheitlich zu übertragen und auszutauschen.
    c) Die Daten werden als sogenannte Ressourcen gespeichert und ausgetauscht und die einzelnen Ressourcen haben Attribute. Die Ressourcen können miteinander verknüpft sein.
    d) Diese Systeme sind meist von verschiedenen Entwicklern und Anbietern, damit die verschiedenen Softwaresysteme trotzdem miteinander kommunizieren können und Daten austauschen können, müssen sie kompatibel aufgebaut sein. Deshalb braucht man Standards, um sicherzustellen, dass trotz unterschiedlicher Systeme die Daten ausgetauscht werden können.
    e) Datenaustausch: FHIR verwendet kompakte, in sich geschlossene Datenpakete, mit einheitlichem, wohldefiniertem Verhalten, Semantik, Kontext- und Metadaten.

11) Welche Protokolle gibt es, die ähnlich wie FHIR sind? Argumentiere, warum FHIR statt diesen verwendet wird.
    a) FHIR Alternativen
        i) HL7 v2
            (1) Datenaustausch syntaktisch & teils semantisch definiert
            (2) Dient vorwiegend dem Datenaustausch innerhalb eines Krankenhauses zwischen KIS, LIS, RIS
            (3) V2 Nachricht besteht aus mehreren Segmenten
            (4) Segmente bestehen aus Feldern mit Datentyp & Bedeutung (Semantik)
        ii) HL7 v3
            (1) XML basiert
            (2) Neuer Ansatz: RIM Reference Information Model
                (a) Davon leiten sich nach Regeln Domäneninformationsmodelle ab.
                (b) Beispiele für Domänen Informationsmodelle: Patientenaufnahme, Terminvergabe, Verschreibung von Medikamenten, etc.
            (3) Daraus ergeben Strukturen für Dokumente und Nachrichten, die ausgetauscht werden können
            (4) Nachrichten und Dokumente können auf Gültigkeit geprüft werden
                (a) XML-Schema
                (b) Schematron
            (5) XML-Schema und Schematron werden ebenfalls aus den Modellen generiert und von HL7 veröffentlicht
            (6) V3 löst derzeit v2 für Kommunikation in KH nicht ab.
        iii) HL7 v3 - CDA (Clinical Document Architecture)
            (1) Basiert auf RIM
            (2) Standard für Datenaustausch zwischen Krankenhäusern, dem niedergelassenen Bereich, etc.
            (3) Besteht aus

(a) Header mit Identifikationsdaten zu Patienten, Behandelndem, Verwaltungsinformationen
(b) und Body mit den tats chlichen Daten

b) Warum FHIR?
   i) FHIR eignet sich für den Datenaustausch besser geeignet
      (1) HL7 v2 → nur vorwiegend für den Datenaustausch zwischen KIS, LIS und RIS ist, in einem Krankenhaus aber es mehr IS gibt.
      (2) HL7 v3 CDA → ist für die Kommunikation zwischen KH und externen IS zuständig
      (3) HL7 v3 → verwendet für den Datenaustausch nur XML, was sehr unpraktisch ist (schwer zu lesen) JSON eignet sich da besser.
   ii) Des Weiteren auch besser für den Anwendungsbereich
      (1) Innerhalb einer Organisationseinheit (z.B. APIS)
      (2) zwischen Organisationseinheiten (APIS, KIS, LIS, RIS)
      (3) zwischen mobiler Anwendung und Organisationseinheit
      (4) Social Web (Patienten Interaktion)
c) FHIR beinhaltet alles in einem, was die Performance von Informationssystemen steigert.

12) Argumentiere, welche Elemente unserer Applikation dem FHIR Standard entsprechen müssen. Warum genau diese und welche nicht? (Z.B. Datenbank, Übertragene Daten zwischen Client, Server, Oberfläche, Modelklassen, ...)
   a) Die Schnittstelle am Server muss dem FHIR-Standard entsprechen und wird durch den Controller umgesetzt. Die Modellklassen definieren einerseits die DB-Struktur, andererseits die JSON Struktur. Die JSON Struktur muss genau dem FHIR Standard entsprechen, das DB-Schema kann davon abweichen. Auch bei den Wertebereichen der Daten gibt FHIR Vorgaben, die z.B. bei der import.sql beachtet werden müssen. Bei der Oberfläche ist die Implementierung des Standards nur implizit durch die dahinterliegende Struktur des FHIR Standards gegeben, aber hier kann auch variiert werden. Die http(s) Kommunikation ist vorgegeben, die Struktur kann JSONoder XML sein.

13) Argumentiere warum es sinnvoll ist, den FHIR Standard einzusetzen.
   a) Der FHIR Standard ermöglicht die Kompatibilität zwischen Systemen im medizinischen Bereich. Im Gesundheitssystem sollte es den Datenaustausch einfach ermöglichen.
   b) Einfache Implementierung durch standardisierte Webtechnologien
   c) Zukunftsrelevanter Standard, weil neu
   d) Einfache Umsetzung mobiler Clients Patienten Apps

14) Beschreibe, welche Anwendungen durch FHIR für Endanwender (Patienten) ermöglicht werden?
    a) FHIR gibt eine Alternative zu Dokumenten zentrierten Ansätzen, in dem es den direkten Zugriff auf einzelne Informationsfelder als Service zulässt. Ein wesentliches Ziel von FHIR ist es, Gesundheitsdaten auch auf mobilen Endgeräten wie Tablet und Smartphone verarbeiten zu können und diese auf einfache Art und Weise in existierende Systeme einzubinden.
    b) Der FHIR Standard wird verwendet, um dem Patienten die Möglichkeit zu geben auf deren Patientendaten zugreifen zu können.
    c) Patientendaten aufzeichnen und dem Arzt zur Verfügung stellen
    d) Der Patient kann mit einem Internetfähigen Device auf seine Gesundheitsdaten zugreifen, spricht der Patient kann jeder Zeit seine Daten aufrufen oder teilen.

15) Zähle zwei Beispiele für einen sinnvollen Einsatz von FHIR auf. Wo wird dabei FHIR eingesetzt?
    a) In einem Krankenhaus kann man den FHIR Standard einsetzen, um die Kommunikation zwischen dem System der Geräte und dem KIS zu gewährleisten. Allgemein ist das Protokoll dafür da, den Datenaustausch zwischen den beiden Systemen sicherzustellen und an dieser Stelle kommt er auch zum Einsatz.
    b) Der Standard kann aber auch für die Kommunikation zwischen dem Melde- und Impfregister in Österreich gewährleisten. Somit kann man sehen, wo die Menschen ohne Schutzimpfung leben und die Systeme sind miteinander verknüpft. Der datenaustausch erfolgt somit auf nationaler Ebene und FHIR kommt einmal mehr bei der Kommunikation zum Einsatz.
    c) Einrichtungs-interne Interoperabilität => Beschreibung überall
    d) Einrichtungsübergreifende Kommunikation
    e) Abrechnungsrelevante Daten für die Krankenkasse
    f) Regionale und nationale Netzwerke z.B.: ELGA, KIS, RIS?
    g) Mobile Applikationen
    h) Social Web (Patienten-Interaktion)

16) Analysiere, wie unsere Applikation serverseitig abgesichert ist?
    a) Die REST Schnittstelle ist ungesichert
    b) DB und Server im gleichen Netz - nicht sicher
    c) DB nur mit Passwort gesichert
    d) Gegen SQL Injections geschützt - weil keine SQL-Statements -
    e) Repository

17) Welche Angriffsmöglichkeiten gibt es und welche Schwachstellen haben wir am Server?
    a) Schwachstellen:
        i) kein HTTPS zwischen Client und Server (Daten sind nicht verschlüsselt → jeder kann mitlesen) → Sicherheitslücke (DB Verbindung ist verschlüsselt)
        ii) kein Login
        iii) Daten manipulierbar über REST Schnittstelle
    b) Angriffsmöglichkeiten:
        i) Datenmanipulation über REST Schnittstelle
        ii) Zugriff auf DB über geratenes PW (Bruteforce)
        iii) SQL-Injection → wir haben keine SQL-Injection weil wir keine SQL-Statements schreiben → das ist gut

18) Welche Maßnahmen wären sinnvoll, um unsere Applikation abzusichern?
    a) Zunächst wäre die Einspielung von Sicherheitszertifikaten wie HTTPS sinnvoll, um die Sicherheit des Datenaustauschs zwischen Client und Server zu erhöhen. Weiters sollte ein Authentifizierungsmodell implementiert werden, welches den Zugriff auf die Ressourcen nur für berechtigte Personen gewährleistet (z.B. 2-Faktor-Authentifizierung). Eine weitere Maßnahme wäre, dass der Server und die Datenbank nicht lokal auf einem Endgerät läuft, sondern sich die Business Logik in einem sicheren Rechenzentrum abspielt. Zuständige Mitarbeiter könnten dann über einen VPN-Konzentrator auf einen Terminal-Server zugreifen und Arbeiten von extern durchführen. Außerdem sollte das Password der Datenbank sich nicht im Code befinden, sondern als Hashwert abgespeichert sein. Die einzelnen Knoten sollte je nach Zusammengehörigkeit in eigene Netzwerke gegliedert werden (Network Separation) um im Falle von Schadsoftware zu gewährleisten, dass nicht gleich das gesamte System verseucht ist. Um Portale unseres APIS zu schützen, sollte eine Firewall konfiguriert werden, die die Server von extern schützt. Für den Schutz von REST-Schnittstellen sollte ein API Gateway eingespielt werden, welches sich unteranderem auch um die Zugriffskontrolle kümmert (rollenbasierte Zugriffsautorisierung). Durch die Verwendung von Hibernate wird bereits gewährleistet, dass Platzhalter für die Eingabewerte verwendet werden. Diese werden anschließend beim Ausführen von Abfragen befüllt und verhindern somit Manipulationen im SQL-Code.
    b) HTTPs - Zertifikat zw. Client und Server
    c) Zertifikate zur DB ○ Authentifizierung und Autorisierung implementieren
    d) Sicheres PW für die DB
    e) Verschiedene Netzwerke zw. DB und Server
    f) Netzwerksicherheit z.B. reverse Proxy siehe Unterricht Hoheiser
    g) Hibernate wird bereits verwendet Bei der Verwendung von Hibernate hat man die Möglichkeit Platzhalter für die Eingabewerte zu verwenden. Diese werden dann beim Ausführen oder Vorbereiten der Abfrage mit den Werten befüllt und blockieren mögliche Manipulationen am SQL-Code.
    h) Gegen physischen Zugriff schützen