



---

## **PROJETO (PART 3)**

---

November 29, 2017

Mariana Galrinho 81669  
Paulo Eusébio 81607  
Renato Henriques 81588

Grupo 15 - SIBD  
Instituto Superior Técnico

## 1. PROCURAR E REGISTAR PACIENTES:

### 1.1 Ficheiro clientPatient.html:

A página inicial corresponde ao ficheiro *checkPatient.html* e consiste numa barra de procura onde se pode escrever o nome, ou parte do nome, de um Paciente que se deseja encontrar na base de dados.

O botão *Submit* reencaminha para a página com a lista de pacientes e a informação do formulário é passada para esta página pelo método POST. Neste projeto todos os formulários utilizam o método POST, uma vez que não há em necessidade de guardar informação em cache, nem de passar dados pelo URL da página.

```
<html>
<head>
  <title>Question 1</title>
  <link href="https://fonts.googleapis.com/css?family=Indie+Flower" rel="stylesheet">
</head>
<body>
  <h1 style="font-family: 'Indie Flower', cursive;">Clinic Database:</h1>

  <form action="listPatients.php" method="post">
    <fieldset style="width: 40%;">
      <legend><strong>Insert the name of the patient:</strong></legend>
      <input type="text" name="Name" autofocus style="width: 80%;" placeholder="Name of patient" />
      <input type="submit" value="Submit"/>
    </fieldset>
  </form>

</body>
</html>
```

Clinic Database:

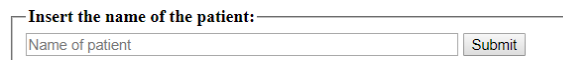


Figure 1: Print da página inicial checkPatient.html

### 1.2 Ficheiro listPatients.php:

Neste ficheiro são apresentados os resultados da pesquisa pelo nome do paciente no ficheiro *checkPatient.html*. A tabela é composta pela informação dos pacientes, nomeadamente, o seu nome, número de identificação, data de nascimento e morada (figure 2). A query utilizada para obter os dados pacientes a partir de parte do seu nome foi "SELECT \* FROM Patient where name like %portion\_name%".

O nome dos pacientes é um link para o seu histórico de utilização de aparelhos (relacionado com a questão 2). Para além disso, incorporou-se na tabela um botão para registar novos Studies para cada paciente (relacionado com a questão 3) e um botão para inserir novas Regions a um elemento de uma série paciente dessa linha (relacionado com a questão 4). Optou-se por colocar estes botões para cada paciente, associando assim, já à partida um paciente a cada nova inserção de um Study ou de uma Region, de forma a tornar a página mais representativa de uma situação real.

Caso a pesquisa não retorne nenhum resultado, ou seja, não haja nenhum paciente com o nome requisitado, então é apresentado um formulário de registo de novo paciente, Figura(3). Optou-se por impedir que o formulário seja submetido com o campo *Number* em branco (tornando obrigatório o seu preenchimento através do parâmetro *Required* do formulário), uma vez que este atributo corresponde à primary key do Patient na base de dados.

De forma a prevenir SQL Injection recorreu-se ao uso de Prepared Statements. Recorrendo à função *prepare*, o programa sabe o tipo de query ou insert que devia receber, o que impossibilita que seja enviados comandos indesejados para a base de dados.

```
<!DOCTYPE html>
<html>
<head>
  <title>Results Question 1:</title>
  <link href="https://fonts.googleapis.com/css?family=Indie+Flower" rel="stylesheet">
```

```
</head>
<body>
  <h1 style="font-family: 'Indie Flower', cursive;">Clinic Database:</h1>

  <?php
    ini_set('display_errors', '0n');
    error_reporting(E_ALL);

    $host = "db.tecnico.ulisboa.pt";
    $user = "istXXXX";
    $pass = "XXXXXXXX";
    $dsn = "mysql:host=$host;dbname=$user";

    try {
      $connection = new PDO($dsn, $user, $pass);
    } catch(PDOException $exception) {
      echo("<p>Error: ");
      echo($exception->getMessage());
      echo("</p>");
      exit();
    }

    $name = $_REQUEST['Name'];

    // SQL Injection Prevention
    $stmt = $connection->prepare("SELECT * FROM Patient where name like CONCAT('%', :portion_name, '%')");

    $stmt->bindParam(':portion_name', $name);
    $stmt->execute();

    if ($stmt == FALSE) {
      $info = $stmt->errorInfo();
      echo("<p>Error: {$info[2]}</p>");
      exit();
    }

    $nrows = $stmt->rowCount();

    // in case of not finding a patient with that name
    // can register a new patient
    if ($nrows == 0) {

      echo("<p>Sorry, patient wasn't found on the database.</p>");

      echo("<form action='newpatient.php' method='post'>");
      echo("<fieldset> <legend><strong>Insert new patient</strong></legend>");
      echo("<p>name: <input type='text' name='name' /></p>");
      echo("<p>number: <input type='text' name='number' required /></p>");
      echo("<p>birthday: <input type='text' name='birthday' /></p>");
      echo("<p>address: <input type='text' name='address' /></p>");
      echo("<p><input type='submit' value='Submit' /></p>");
      echo("</fieldset>");
      echo("</form>");

      // prints a table with the results
    } else {
      echo "<h3>Results Found:</h3>";
      echo("<table border='1' cellspacing='5'>");
      echo("<tr><td><strong>Name</strong></td><td><strong>ID</strong></td><td><strong>Region</strong></td></tr>");
      echo("<tr><td><strong>Number</strong></td><td><strong>Birthday</strong></td><td><strong>Address</strong></td></tr>");

      foreach($stmt as $row) {
        echo("<tr><td>");
        echo("<a href='listDevices.php?number='");
        echo($row['number']");
        echo("</a>");
        echo("</td><td>");
        echo($row['number']");
        echo("</td><td>");
        echo($row['birthday']");
        echo("</td><td>");
        echo($row['address']");
        echo("</td><td>");
        echo("<a href='formRegions.php?number='");
        echo($row['number']");
        echo("</a>");
        echo("<button type='button'>Insert</button></a>");
        echo("</td></tr>");
      }

      echo("</table>");
    }

    // Button to go to home page
    echo("<br><form action='checkPatient.html' method='post'>");
    echo("<input type='submit' value='Home' /></form>");

    $connection = null;
  ?>
</body>
</html>
```

## Clinic Database:

Results Found:

Name	ID number	Birthday	Address	Study	Region
<a href="#">Ruben</a>	1	1995-02-25	Av. do Tecnico	<a href="#">Register</a>	<a href="#">Insert</a>
<a href="#">Andre</a>	2	1912-04-15	Rua oliveirinha	<a href="#">Register</a>	<a href="#">Insert</a>
<a href="#">Francisco</a>	6	1989-12-19	Av. da Liberdade	<a href="#">Register</a>	<a href="#">Insert</a>
<a href="#">Salazar</a>	666	1889-04-28	Santa Comba Dão	<a href="#">Register</a>	<a href="#">Insert</a>
<a href="#">Dimitri</a>	1235	0666-10-10	Russia	<a href="#">Register</a>	<a href="#">Insert</a>
<a href="#">Vitor</a>	10811	1887-12-01	Alvalade	<a href="#">Register</a>	<a href="#">Insert</a>
<a href="#">Mariana</a>	18012	1999-01-23	Valverde	<a href="#">Register</a>	<a href="#">Insert</a>
<a href="#">Fedra</a>	27233	1987-11-25	Cova da Moura	<a href="#">Register</a>	<a href="#">Insert</a>
<a href="#">Rita</a>	187529	1987-01-25	Lourel	<a href="#">Register</a>	<a href="#">Insert</a>
<a href="#">Erika</a>	199456	2001-12-20	La Street	<a href="#">Register</a>	<a href="#">Insert</a>
<a href="#">Marcelo</a>	851015	1942-12-02	Cascais	<a href="#">Register</a>	<a href="#">Insert</a>
<a href="#">Ruben</a>	9256926	1991-03-30	Benfica	<a href="#">Register</a>	<a href="#">Insert</a>
<a href="#">Renato</a>	913641308	1996-02-23	Rua do zé	<a href="#">Register</a>	<a href="#">Insert</a>

[Home](#)

**Figure 2:** listPatients.php - Caso em que são encontrados pacientes com o nome requisitado (neste caso que possuem a letra r no nome).

## Clinic Database:

Sorry, patient wasn't found on the database.

**Insert new patient**

name:

number:

birthday:

address:

[Home](#)

**Figure 3:** listPatients.php - Caso em que não é encontrado nenhum paciente com o nome requisitado.

## 1.2 Ficheiro newpatient.php:

Depois de preencher-se o formulário para registar um novo paciente, executa-se o código PHP do ficheiro *newpatient.php* para inserir o novo paciente na base de dados. Optou-se por incluir uma mensagem que transmita o resultado da inserção, apresentando uma mensagem de erro, caso haja impedimentos na inserção, ou todos os dados que foram inseridos, caso a inserção seja efetuada com sucesso.

```
<?php
$host = "db.tecnico.ulisboa.pt";
$user = "istxxxxxz";
$pass = "xxxxxxx";
$dns = "mysql:host=$host;dbname=$user";

try {
    $connection = new PDO($dns, $user, $pass);
} catch(PDOException $exception) {
    echo("<p>Error: ");
    echo($exception->getMessage());
    echo("</p>");
    exit();
}

$name = $_REQUEST['name'];
$number = $_REQUEST['number'];
$birthday = $_REQUEST['birthday'];
$address = $_REQUEST['address'];

$stmt = $connection->prepare("INSERT INTO Patient VALUES (:number, :name, :birthday, :address)");

$stmt->bindParam(':name', $name);
$stmt->bindParam(':number', $number);
```

```

$stmt->bindParam(':birthday', $birthday);
$stmt->bindParam(':address', $address);

$result = $stmt->execute();

if ($result == 0){
    $info = $stmt->errorInfo();
    echo("<p> Error, the insertion was not successful: {$info[2]}</p>");
} else {
    echo("<p> New patient was inserted successfully. </p>");

    echo("<table border='1' cellspacing='5'>");
    echo("<tr><td><strong>Name</strong></td><td><strong>ID number</strong></td><td><strong>Birthday</strong></td><td><strong>Address</strong></td></tr>");
    echo("<tr>");
    foreach($_REQUEST as $value) {
        echo("<td>");
        echo($value);
        echo("</td>");
    }
    echo("</tr>");
    echo("</table><br>");
}

echo("<form action='checkPatient.html' method='post'>");
echo("<input type='submit' value='Home'></form>");

$conn = null;
?>

```

New patient was inserted successfully.

Name	ID number	Birthday	Address
Isabel	588	1995-02-25	Lisboa

Home

**Figure 4:** newpatient.php - Caso em que um novo paciente é inserido com sucesso na base de dados.

## 2. ALTERAÇÃO DOS APARELHOS CONECTADOS AO PACIENTE:

### 2.1 Ficheiro listDevices.php:

Na procura de um *Patient*, para a lista de resultados apresentados, cada nome contém um link para a página *listDevices.php*, em que é enviado (por URL) o ID do patient (que o identifica unicamente), que mostra todos os *devices* usados por ele. Caso o paciente esteja a usar algum *device*, é apresentado um botão que permite substituí-lo.

Foi necessário guardar a informação do paciente e do seu *device* (por URL), já que a lista de possíveis substituições deve mostrar apenas os *devices* disponíveis do mesmo fabricante. Os *devices* que estão a ser usados pelo paciente no momento em que é feita a *query* são realçados, isto é, caso a data final seja superior à data atual é colocado a negrito o *manufacturer* e o seu *serial number*. A *query* feita para encontrar os *devices*, ordena-os por data final do uso, de forma decrescente, permitindo apresentar no topo da tabela de resultados os *devices* que estão a ser usados no momento.

```

<!DOCTYPE html>
<html>
<head>
    <title>Device of patient</title>
    <link href="https://fonts.googleapis.com/css?family=Indie+Flower" rel="stylesheet">
</head>
<body>
    <h1 style="font-family: 'Indie Flower', cursive;">Clinic Database:</h1>

    <?php
        ini_set('display_errors', 'On');
        error_reporting(E_ALL);

        $host = "db.tecnico.ulisboa.pt";
        $user = "istXXXXXX";
        $pass = "XXXXXXXXX";
        $dsn = "mysql:host=$host;dbname=$user";

        try {
            $connection = new PDO($dsn, $user, $pass);
        } catch(PDOException $exception) {
            echo("<p>Error: ");
            echo($exception->getMessage());
        }
    </?php>

```

```

        echo("</p>");
        exit();
    }

    $idnumber = $_REQUEST['number'];

    echo("<h3>List of devices worn by Patient nr. " . $idnumber . " :</h3>");

    $stmt = $connection->prepare("SELECT snum, manuf, start, end FROM Wears where patient = :idnumber order by end desc ");
    $stmt->bindParam(':idnumber', $idnumber);
    $result = $stmt->execute();

    if ($result == FALSE) {
        $info = $stmt->errorInfo();
        echo("<p>Error: {$info[2]}</p>");
        exit();
    }

    $nrows = $stmt->rowCount();
    if ($nrows == 0) {
        echo("<p>Patient haven't worn any device.</p>");
    } else {
        echo("<table border='1' cellspacing='5'>");
        echo("<tr><td><strong>Serial Number</strong></td><td><strong>Manufacturer</strong></td><td><strong>Start Date</strong></td><td><strong>End Date</strong></td></tr>");
        foreach($stmt as $row) {
            if ( strcmp($row['end'], date("Y-m-d H:i:s",time())) > 0){
                echo("<tr><td><strong>");
                echo($row['snum']);
                echo("</strong></td><td><strong>");
                echo($row['manuf']);
                echo("</strong></td><td>");
                echo($row['start']);
                echo("</td><td>");
                echo($row['end']);
                echo("</td>");
                echo("<td><a href='listReplacements.php?patient='");
                echo($idnumber . "&serialnum='");
                echo($row['snum'] . "&manufacturer='");
                echo($row['manuf']");
                echo("><button type='button'>Replace</button></a></td>");
            } else {
                echo("<tr><td>");
                echo($row['snum']);
                echo("</td><td>");
                echo($row['manuf']);
                echo("</td><td>");
                echo($row['start']);
                echo("</td><td>");
                echo($row['end']);
                echo("</td>");
            }
            echo("</tr>");
        }
        echo("</table>");
    }

    // Button to go to home page
    echo("<br><form action='checkPatient.html' method='post'>");
    echo("<input type='submit' value='Home'></form>");

    $connection = null;
?>
</body>
</html>

```

### Clinic Database:

#### List of devices worn by Patient nr. 7465:

Serial Number	Manufacturer	Start Date	End Date	
3000	Medtronic	2017-11-27 15:17:51	2999-12-31 00:00:00	Replace
1297419	Siemens	2017-11-27 10:20:17	2999-12-31 00:00:00	Replace
1000	Medtronic	2017-11-25 22:42:24	2017-11-27 15:17:51	
20	Siemens	2017-11-23 18:14:26	2017-11-27 10:20:17	
3000	Medtronic	2017-11-23 11:50:19	2017-11-25 22:42:24	
1297419	Siemens	2017-11-22 22:16:28	2017-11-23 18:14:26	
3333	Medtronic	2017-11-22 22:18:28	2017-11-23 11:50:19	
3000	Medtronic	2017-11-22 22:17:02	2017-11-22 22:18:28	
3333	Medtronic	2017-02-02 14:00:00	2017-11-22 22:17:02	
5224	Siemens	2013-02-15 11:22:00	2017-11-22 22:16:28	
4552	Samsung	2009-03-11 10:11:00	2010-03-21 08:11:00	

[Home](#)

**Figure 5:** listDevices.php - Histórico de devices de um paciente.

Pela figura 5, o paciente usa atualmente dois *devices* que estão realçados e é oferecida a possibilidade de

substituir qualquer um pelo botão *replace*. Caso o paciente nunca tenha usado um device será imprimida uma mensagem com essa informação.

## 2.2 Ficheiro listReplacements.php

Ao clicar no botão *replace* o utilizador é reencaminhado para a página *listReplacements.php* que mostra os *devices* do mesmo fabricante, disponíveis naquele momento. Recorre-se a uma *sub-query* que recolhe todos os *devices* a ser utilizados no presente momento. Os resultados apresentados pela *query* são todos os *devices* desse fabricante que não aparecem na *sub-query*, ou seja, os *devices* do fabricante pedido que nunca foram usados ou que foram usados no passado mas não no presente.

```
<!DOCTYPE html>
<html>
<head>
  <title>Replace Device:</title>
  <link href="https://fonts.googleapis.com/css?family=Indie+Flower" rel="stylesheet">
</head>
<body>
  <h1 style="font-family: 'Indie Flower', cursive;">Clinic Database:</h1>

<?php
  ini_set('display_errors', 'On');
  error_reporting(E_ALL);

  $host = "db.tecnico.ulisboa.pt";
  $user = "istXXXXXX";
  $pass = "XXXXXXXXX";
  $dsn = "mysql:host=$host;dbname=$user";

  try {
    $connection = new PDO($dsn, $user, $pass);
  } catch(PDOException $exception) {
    echo("<p>Error: ");
    echo($exception->getMessage());
    echo("</p>");
    exit();
  }

  $idnumber = $_REQUEST['patient'];
  $devId = $_REQUEST['serialnum'];
  $manuf = $_REQUEST['manufacturer'];

  // Select all the devices that aren't being worn at the moment
  $stmt = $connection->prepare("SELECT serialnum, model FROM Device as d WHERE manufacturer = :manuf and serialnum not in (SELECT snum FROM Wears WHERE manuf = :manuf
    and timediff(Wears.end, NOW()) > 0)");

  $stmt->bindParam(":manuf", $manuf);

  $result = $stmt->execute();
  if ($result == FALSE) {
    $info = $stmt->errorInfo();
    echo("<p>Error: {$info[2]}</p>");
    exit();
  }

  echo("<h3>Devices of manufacturer <i>{$manuf}</i> available for replacement:</h3>");

  $nrows = $stmt->rowCount();
  if ($nrows == 0) {
    echo("<p>No device available at the moment.</p>");
  } else {
    echo("<table border='1' cellspacing='5'>");
    echo("<tr><td><strong>Serial Number</strong></td><td><strong>Model</strong></td></tr>");
    foreach($stmt as $row) {
      echo("<tr><td>");
      echo($row['serialnum']);
      echo("</td><td>");
      echo($row['model']);
      echo("</td><td>");
      //BUTTON THAT UPDATES THE WEARS VALUE
      echo("<a href='updateDevice.php?patient='");
      echo($idnumber . '&numOld=');
      echo($devId . '&manuf=');
      echo($manuf . '&numNew=');
      echo($row['serialnum']);
      echo("><button type='button'>Change</button></a>");
      echo("</td></tr>");
    }
    echo("</table>");
  }

  // Button to go to home page
  echo("<br><form action='checkPatient.html' method='post'>");
  echo("<input type='submit' value='Home' /></form>");

  $connection = null;
?>

</body>
</html>
```

## Clinic Database:

Devices of manufacturer *Medtronic* available for replacement:

Serial Number	Model	
1000	Adidas	<input type="button" value="Change"/>
31	scanner	<input type="button" value="Change"/>
3333	GlucoseReader	<input type="button" value="Change"/>
443	BloodReader	<input type="button" value="Change"/>

Figure 6: listReplacements.php - Alternativas para um device Medtronic.

A figura 6 mostra as alternativas para substituir um *device* do fabricante *medtronic* que estão disponíveis naquele momento. É apresentado um botão *change* que permite substituir a informação na base de dados.

## 2.3 Ficheiro updateDevice.php:

Para efetuar a mudança, o utilizador clica no botão *change* que reencaminha para o ficheiro *updateDevice.php*, a informação necessária é enviada por URL.

Pretende-se que o paciente que usa o *device X* comece a usar o *device Y*. Para isso é necessário alterar a data final de *X* para a data atual e criar uma nova linha na relação *Wears* para *Y* com data de início igual à data atual e data final indefinida. Também foi necessário acrescentar as datas à entidade *Period*, contudo como estas inserções não dependem de entradas externas à base de dados, não foi necessário implementar mecanismos de prevenção de SQL Injection. Caso não haja *devices* disponíveis é apresentada uma mensagem com essa informação.

```
<!DOCTYPE html>
<html>
<head>
<title>Update Device:</title>
</head>
<body>
<?php
    $host = "db.tecnico.ulisboa.pt";
    $user = "istXXXXXX";
    $pass = "XXXXXXXXX";
    $dsn = "mysql:host=$host;dbname=$user";

    try {
        $connection = new PDO($dsn, $user, $pass);
    } catch(PDOException $exception) {
        echo("<p>Error: ");
        echo($exception->getMessage());
        echo("</p>");
        exit();
    }

    $patientid = $_REQUEST['patient'];
    $snumOld = $_REQUEST['snumOld'];
    $manuf = $_REQUEST['manuf'];
    $snumNew = $_REQUEST['snumNew'];

    $stmt = $connection->prepare("SELECT start, end FROM Wears WHERE patient = :patientid and snum = :snumOld and manuf = :manuf and timediff(end, NOW()) > 0");

    $stmt->bindParam(':patientid', $patientid);
    $stmt->bindParam(':snumOld', $snumOld);
    $stmt->bindParam(':manuf', $manuf);

    $result = $stmt->execute();

    if ($result == FALSE) {
        $info = $stmt->errorInfo();
        echo("<p>Error query dates:{info[2]}</p>");
        exit();
    }

    $row = $stmt->fetch();
    $start_date = $row['start'];
    $end_date = $row['end'];

    // We want that the update and the insertion to be done simultaneously
    $connection->beginTransaction();

    // Insert two new periods in the Period table, one for the old device and for the new
    // we use this variable because the function time() can give two different results
    $current_date = date("Y-m-d H:i:s");
    $sql = "Insert into Period values ('$start_date', '$current_date'); Insert into Period values('$current_date', '$end_date');";
    $result = $connection->exec($sql);
```



```

if ($result == FALSE) {
    $info = $connection->errorInfo();
    echo("<p>Error: {$info[2]}</p>");
    exit();
}

// UPDATING THE END DATE OF THE OLD DEVICE
$stmt1 = $connection->prepare("UPDATE Wears SET end = :now_date WHERE patient = :patientid and snum = :snumOld and manuf = :manuf and start = :start_date and end = :end_date");

$stmt1->bindParam(':now_date', $current_date);
$stmt1->bindParam(':patientid', $patientid);
$stmt1->bindParam(':snumOld', $snumOld);
$stmt1->bindParam(':manuf', $manuf);
$stmt1->bindParam(':start_date', $start_date);
$stmt1->bindParam(':end_date', $end_date);

// INSERTING THE NEW WEARABLE DATA
$stmt2 = $connection->prepare("INSERT INTO Wears VALUES (:now_date,:endDate,:patientid,:snumNew, :manuf)");

$stmt2->bindParam(':now_date', $current_date);
$stmt2->bindParam(':endDate', $end_date);
$stmt2->bindParam(':patientid', $patientid);
$stmt2->bindParam(':snumNew', $snumNew);
$stmt2->bindParam(':manuf', $manuf);

if ($stmt1->execute() && $stmt2->execute()){
    $connection->commit();

    echo("<p>Success, replacement was successful.</p>");
} else {
    $connection->rollBack();
    echo("<p>Replacement wasn't successful.</p>");
    echo 'Error executing statement: ' . $stmt1->errorInfo()[2] . ' ' . $stmt2->errorInfo()[2] ;
}

// Button to go to home page
echo("<br><form action='checkPatient.html' method='post'>");
echo("<input type='submit' value='Home'/></form>");

$connection = null;
?>
</body>
</html>

```

Success, replacement was successful.

Home

Figure 7: updateDevice.php - Histórico de devices de um paciente.

Ao fazer *update* é mostrada uma mensagem que indica sucesso ou falha. Caso se pretenda visualizar as alterações efetuadas basta utilizar o botão home para voltar a procurar o nome do paciente e visualizar novamente os seus devices.

Optou-se for fazer uma *transaction* quando se muda um *device*, uma vez que envolve alterações em várias tabelas, logo é necessário garantir que são todas atualizadas com sucesso. Todas as comunicações com a base de dados dependentes de variáveis inseridas pelo utilizador são pré-preparadas contra *SQL injection*.

### 3. CRIAÇÃO DE NOVOS STUDIES E SERIES:

#### 3.1. Ficheiro formStudy.php

É pedido nesta questão para criar um novo Study e, em simultâneo, criar um novo Series. Estas duas novas inserções na base de dados devem ser efetuadas juntas, ou seja, numa única transação.

Para obter o número de identificação do paciente ao qual se pretende criar o registo do Study colocou-se um botão que reencaminha para a página *formStudy.php* e envia pelo URL o número do paciente.

Ao abrir a página *formStudy.php* podem acontecer um dos seguintes eventos:

- O paciente não tem nenhum Request associado à sua identificação. Nesse caso, não existe uma forma de criar um Study associado a este paciente e na página aparece uma mensagem de aviso sobre este acontecimento. Não foi implementada uma forma de criar um novo Request para o paciente (não foi pedido no enunciado do projeto), de modo que para efetuar esta alteração é necessário inserir diretamente pela consola do MySQL.

- O paciente tem um Request associado ao seu número de identificação. Para este caso, na página *form-Study.php* é carregado um formulário para a criação de um novo Study.

O formulário para a criação de um novo Study é composto pelos seguintes elementos: uma lista Drop-down que apresenta todos os Request Numbers associados aquele paciente, os restantes atributos do Study (Sendo que o request number e a description são parâmetros obrigatórios já que correspondem a primary keys) e o nome e identificação da Series que se pretende criar (também parâmetros obrigatórios).

```
<html>
<head>
  <title>Create a new study:</title>
  <link href="https://fonts.googleapis.com/css?family=Indie+Flower" rel="stylesheet">
</head>
<body>
  <h1 style="font-family: 'Indie Flower', cursive;">Clinic Database:</h1>

  <form method="post" action="createStudy.php">
    <fieldset style="width: 50%;">
      <legend><strong>Register a new Study:</strong></legend>

<?php
    $host = "db.ist.utl.pt";
    $user = "ist181588";
    $pass = "gjfz1955";
    $dsn = "mysql:host=$host;dbname=$user";
    try
    {
        $connection = new PDO($dsn, $user, $pass);
    }
    catch(PDOException $exception)
    {
        echo("<p>Error: ");
        echo($exception->getMessage());
        echo("</p>");
        exit();
    }

    $stmt = $connection->prepare("SELECT number FROM Request where patient_id=patient_id ORDER BY number");
    $stmt->bindParam(':patient_id', $_REQUEST['number']);

    $result = $stmt->execute();
    if ($result == 0){
        $info = $stmt->errorInfo();
        echo("<p> Query Error: {$info[2]}</p>");
        exit();
    }

    if($stmt->rowCount() == 0){
        echo("<p>There isn't a requested study for this Patient.</p>");

        echo("</fieldset></form>");
        //Button to go to home page
        echo("<br><form action='checkPatient.html' method='post'>");
        echo("<input type='submit' value='Home'></form>");
        $connection = null;
        exit();
    }

    echo("<p><strong>Request Number:</strong>");
    echo("<select name='requestnumber'>");

    foreach($stmt as $row)
    {
        $requestnumber = $row['number'];
        echo("<option value=\"{$requestnumber}\">{$requestnumber}</option>");
    }

    $connection = null;
?>
</select>
</p>
<p><strong>Description:</strong>
<input type="text" name="description" autofocus style="width: 60%;" maxlength="255" placeholder="Description" required /><br></p>
<p><strong>Date:</strong>
<input type="text" name="date" autofocus style="width: 40%;" maxlength="20" placeholder="YEAR-MONTH-DAY"/><br></p>
<p><strong>Doctor ID:</strong>
<input type="text" name="doctorid" autofocus style="width: 40%;" maxlength="30" placeholder="Doctor ID" /></p>
<p><strong>Manufacturer of Device:</strong>
<input type="text" name="manufacturer" autofocus style="width: 50%;" maxlength="255" placeholder="Manufacturer" /></p>
<p><strong>Serial Number of Device:</strong>
<input type="text" name="serialnumber" autofocus style="width: 40%;" maxlength="255" placeholder="Serial Number" /></p>
<p><strong>Series ID:</strong>
<input type="text" name="seriesid" autofocus style="width: 20%;" maxlength="30" placeholder="Series ID" required /><p>
<p><strong>Series Name:</strong>
<input type="text" name="seriesname" autofocus style="width: 20%;" maxlength="30" placeholder="Series Name" /><p>
<input type="submit" value="Submit"/></p>
</fieldset>
</form>

<!-- Button to go to home page -->
<br><form action='checkPatient.html' method='post'>
<input type='submit' value='Home' /></form>
</body>
</html>
```

Clinic Database:

Figure 8: formStudy.php - Formulário de um novo Study.

### 3.2. Ficheiro createStudy.php

Clicando submeter o formulário, o utilizador é encaminhado para a página *createStudy.php* onde é realizada a inserção do novo Study e da nova Series. Tal como foi pedido pelo problema, a inserção dos dois elementos é feita em paralelo. Caso uma das duas operações não seja realizada corretamente, então nenhuma delas é executada. Desta forma, pode-se prevenir a inserção de um Series sem que o Study associado seja criado.

Utilizou-se, novamente, *prepared statements*, uma vez que, como as variáveis das operações Insert têm origem no formulário da página anterior, o programa estaria sujeito a SQL Injection.

Se as duas operações forem bem sucedidas, é feito o commit e é impressa uma mensagem de sucesso, tal como as duas tabelas com a informação que foi inserida com o objetivo de verificar o bom funcionamento da página. Se, por outro lado, uma das operações tenha falhado, então é impressa uma mensagem a dizer que as operações não tiveram sucesso e apresenta o erro.

Como as operações SQL efetuadas na transaction não correspondem a leituras, mas sim inserções, não houve necessidade de alterar o nível de isolamento da transação, ficando assim o default, *repeatable read*.

```
<!DOCTYPE html>
<html>
<head>
  <title>Update Study:</title>
</head>
<body>
  <?php
    ini_set('display_errors', 'On');
    error_reporting(E_ALL);

    $host = "db.tecnico.ulisboa.pt";
    $user = "ist181588";
    $pass = "gjzjf1955";
    $dsn = "mysql:host=$host;dbname=$user";

    try {
      $connection = new PDO($dsn, $user, $pass);
    } catch(PDOException $exception) {
      echo("<p>Error: ");
      echo($exception->getMessage());
      echo("</p>");
      exit();
    }

    $requestnumber = $_REQUEST['requestnumber'];
    $description = $_REQUEST['description'];
    $date = $_REQUEST['date'];
    $doctorid = $_REQUEST['doctorid'];
    $manufacturer = $_REQUEST['manufacturer'];
    $serialnumber = $_REQUEST['serialnumber'];
    $seriesid = $_REQUEST['seriesid'];
    $seriesname = $_REQUEST['seriesname'];

    $base_url = 'http://web.tecnico.ulisboa.pt/' . $user . '/series/' . $seriesid;

    $connection->beginTransaction();

    $stmt1 = $connection->prepare("INSERT INTO Study VALUES (:requestnumber,:description,:date, :doctorid, :manufacturer,:serialnumber)");

    $stmt1->bindParam(':requestnumber', $requestnumber);
    $stmt1->bindParam(':description', $description);
    $stmt1->bindParam(':date', $date);
    $stmt1->bindParam(':doctorid', $doctorid);
    $stmt1->bindParam(':manufacturer', $manufacturer);
    $stmt1->bindParam(':serialnumber', $serialnumber);

    $stmt2 = $connection->prepare("INSERT INTO Series VALUES (:seriesid, :name, :base_url,:requestnumber,:description)");
```

```

// series id is unique!!
$stmt2->bindParam(':seriesid', $seriesid, PDO::PARAM_INT);
$stmt2->bindParam(':name', $seriesname);
$stmt2->bindParam(':base_url', $base_url);
$stmt2->bindParam(':requestnumber', $requestnumber);
$stmt2->bindParam(':description', $description);

if ($stmt1->execute() && $stmt2->execute()){
    $connection->commit();

    echo("<h3>Success, study created.</h3>");

    echo("<p><strong>Study values inserted:</strong></p>");
    echo("<table border='1' cellspacing='5'>");
    echo("<tr><td><strong>Request Number</strong></td><td><strong>Description</strong></td><td><strong>Date</strong></td><td><strong>Doctor ID</strong></td><td><strong>Manufacturer</strong></td><td><strong>Serial Number</strong></td></tr>");
    echo("<tr>");
    echo("<td> $requestnumber </td>");
    echo("<td> $description </td>");
    echo("<td> $date </td>");
    echo("<td> $doctorid </td>");
    echo("<td> $manufacturer </td>");
    echo("<td> $serialnumber </td>");
    echo("</tr>");
    echo("</table><br>");

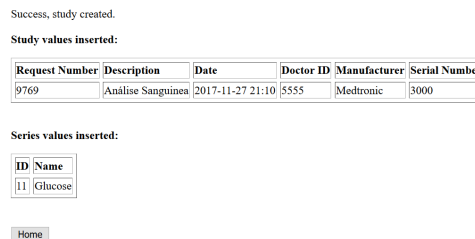
    echo("<p><strong>Series values inserted:</strong></p>");
    echo("<table border='1' cellspacing='5'>");
    echo("<tr><td><strong>ID</strong></td><td><strong>Name</strong></td></tr>");
    echo("<tr>");
    echo("<td> $seriesid </td>");
    echo("<td> $seriesname </td>");
    echo("</tr>");
    echo("</table><br>");

} else {
    $connection->rollBack();
    echo("<p>Study not created.</p>");
    echo "Error executing statement: " . $stmt1->errorInfo()[2] . " " . $stmt2->errorInfo()[2] ;
}

// Button to go to home page
echo("<br><form action='checkPatient.html' method='post'>");
echo("<input type='submit' value='Home'></form>");

$connection = null;
?>
</body>
</html>

```



**Figure 9:** createStudy.php - Inserção do novo Study e Series, mensagens de sucesso ou fracasso.

## 4. ADICIONAR NOVAS REGIONS:

Nesta questão é pedido no enunciado para adicionar uma região a um elemento de uma Series e caso a região inserida não se sobreponha com nenhuma das regiões do último Study do paciente, alertar para a existência de novas evidências clínicas. Posto isto, assumiu-se que a região em questão poderia ser inserida em qualquer um dos Studies já associados a um determinado paciente e que a verificação da sobreposição se efetuava com todas as regiões do último Study (excepto com a própria região caso esta seja inserida no último estudo), isto é, do Study cuja data é a maior das datas de todos os Studies desse paciente.

Optou-se por colocar botões na página com a lista dos pacientes (listPatients.php) associados a cada um dos pacientes, e que permitam inserir novas regiões nas suas respetivas Series. Para tal, passa-se o número de identificação do paciente através do URL, e assim, o formulário onde será inserida a região é referente a cada paciente específico. Outra alternativa seria a criação de um só formulário no qual fosse possível inserir regiões de qualquer paciente, sendo o seu id obtido através de uma query que envolvesse a tabela Request. Porém, e uma vez que para a questão em mãos não faz sentido uma região existir sem que esta esteja associada a um

determinado paciente, optou-se pela primeira implementação.

## 4.1 Ficheiro formRegions.php:

Caso o paciente escolhido tenha pelo menos uma Series para um Study que lhe esteja associado, é apresentado um formulário de inserção de uma nova região. Neste é exibida uma lista drop-down onde figuram todas as Series do paciente, dando assim oportunidade ao utilizador de escolher apenas Series já existentes. Para além disso, os restantes campos necessários à identificação de uma região são de preenchimento obrigatório, uma vez que se tratam de primary keys. Caso não haja nenhuma Series associada ao paciente, então não é possível fazer a inserção de uma nova região, sendo para isso necessário inserir em primeiro lugar pelo menos uma Series através da consola MySQL.

```
<html>
<head>
  <title>Insert Regions:</title>
  <link href="https://fonts.googleapis.com/css?family=Indie+Flower" rel="stylesheet">
</head>
<body>
  <h1 style="font-family: 'Indie Flower', cursive;">Clinic Database:</h1>

  <form method="post" action="insertRegion.php" autocomplete="off">
    <fieldset style="width: 40%;">
      <legend><strong>Add a new region:</strong></legend>

<?php

  $host = "db.tecnico.ulisboa.pt";
  $user = "istxxxxxx";
  $pass = "xxxxxxx";
  $dsn = "mysql:host=$host;dbname=$user";

  try {
    $connection = new PDO($dsn, $user, $pass);
  } catch(PDOException $exception) {
    echo("<p>Error: ");
    echo($exception->getMessage());
    echo("</p>");
    exit();
  }

  $stmt = $connection->prepare("select series_id from Series as s, Request as r where s.request_number = r.number and r.patient_id = :patient_id order by
    series_id asc;");

  $stmt->bindParam(':patient_id', $_REQUEST['number']);

  $result = $stmt->execute();

  if ($result == 0){
    $info = $stmt->errorInfo();
    echo("<p> Query Error: {$info[2]}</p>");
    exit();
  }

  if($stmt->rowCount() == 0){
    echo("<p>There isn't a Series associated with this Patient.</p>");

    echo("</fieldset></form>");
    //Button to go to home page
    echo("<br><form action='checkPatient.html' method='post'>");
    echo("<input type='submit' value='Home'></form>");
    $connection = null;
    exit();
  }

  echo("<p><strong>Series ID:</strong>");
  echo("<select name='seriesid'>");

  foreach($stmt as $row) {
    $seriesid = $row['series_id'];
    echo("<option value=\"\$seriesid\">{$seriesid}</option>");
  }

  $connection = null;

?>
</select>
</p>

<p><strong>Element Index:</strong>
<input type="text" name="elem_index" autofocus style="width: 50%;" maxlength="30" placeholder="Element Index" required /><br></p>
<p><strong>X1:</strong>
<input type="text" name="x1" autofocus style="width: 10%;" maxlength="10" placeholder="x1" required /><br></p>
<p><strong>Y1:</strong>
<input type="text" name="y1" autofocus style="width: 10%;" maxlength="10" placeholder="y1" required /><br></p>
<p><strong>X2:</strong>
<input type="text" name="x2" autofocus style="width: 10%;" maxlength="10" placeholder="x2" required /><br></p>
<p><strong>Y2:</strong>
<input type="text" name="y2" autofocus style="width: 10%;" maxlength="10" placeholder="y2" required /><br></p>
<p><input type="hidden" name="patient_id" value="<?=$_REQUEST['number']?>" /></p>
<p><input type="submit" value="Submit" /></p>
</fieldset>
</form>

<!-- Button to go to home page -->
```

```

<br>
<form action='checkPatient.html' method='post'>
  <input type='submit' value='Home' />
</form>

</body>
</html>

```

### Clinic Database:

**Figure 10:** formRegions.php - Formulário para inserção de uma nova region para o paciente 7465.

## 4.1 Ficheiro insertRegion.php:

A informação preenchida no formulário anterior é utilizada para efetuar a inserção na base de dados e a verificação da sobreposição a partir do ficheiro insertRegion.php. Neste começa-se por obter os valores das coordenadas de cada região associada aos elementos do último estudo efetuado pelo paciente (query com prepared statement stmt1), de forma a obter facilmente um conjunto de regiões no qual esteja excluída a região a ser introduzida (caso esteja seja inserida no último estudo). Após esta query, é realizada a inserção da nova região na base de dados e a comparação com os resultados da query acima, podendo ocorrer três situações distintas:

- Existem problemas durante o processo de inserção da nova região na base de dados. Se assim for, é apresentada uma mensagem de erro e feito exit(), uma vez que não se pretende efetuar mais operações se a região em questão não for corretamente introduzida.
- Não ocorrem erros durante a inserção da nova região mas a query inicial não devolve nenhum resultado. Isto pode acontecer, por exemplo, caso ainda não tenham sido inseridas regiões na Series associadas ao último Study do paciente. Nesta situação, é apresentada uma mensagem a confirmar que a inserção foi efetuada com sucesso mas que não há nenhuma região com a qual efetuar a comparação.
- A região é inserida com sucesso e existem regiões com a qual pode ser comparada. Neste caso, adopta-se uma abordagem semelhante à utilizada na questão 6 do projeto 2 para a verificar se há sobreposição das regiões. Após a comparação com todas as regiões e se não houver nenhuma sobreposição, é apresentada uma mensagem a informar que existem novas evidências clínicas.

```

<html>
<head>
  <title>Insertion of new region</title>
  <link href="https://fonts.googleapis.com/css?family=Indie+Flower" rel="stylesheet">
</head>
<body>
  <h1 style="font-family: 'Indie Flower', cursive;" href="checkPatient.html">Clinic Database:</h1>

  <?php
    $host = "db.tecnico.ulisboa.pt";

    $user = "istxxxxxx";
    $pass = "xxxxxxx";

    $dsn = "mysql:host=$host;dbname=$user";

```

```

try {
    $connection = new PDO($dan, $user, $pass);
} catch(PDOException $exception) {
    echo("<p>Error: ");
    echo($exception->getMessage());
    echo("</p>");
    exit();
}

// get the region info
$series_id = $_REQUEST['seriesid'];
$elem_index = $_REQUEST['elem_index'];
$patient_id = $_REQUEST['patient_id'];
$x1 = $_REQUEST['x1'];
$y1 = $_REQUEST['y1'];
$x2 = $_REQUEST['x2'];
$y2 = $_REQUEST['y2'];

// QUERY -> get all regions of an element from the last study of the patient (if there was one)
$stmt1 = $connection->prepare("select x1,y1,x2,y2 from Region as r, Series as s, Study as st, Request as rq where r.series_id=s.series_id and
s.request_number=st.request_number and s.description=st.description and st.request_number=rq.number and rq.patient_id= :patient_id and st.date >=all
(select st1.date from Study as st1, Request as rq1 where st1.request_number=rq1.number and rq1.patient_id= :patient_id );");

$stmt1->bindParam(':patient_id', $patient_id);
$result1 = $stmt1->execute();

$stmt = $connection->prepare("INSERT INTO Region VALUES (:series_id,:elem_index,:x1,:y1,:x2,:y2)");

$stmt->bindParam(':series_id', $series_id);
$stmt->bindParam(':elem_index', $elem_index);
$stmt->bindParam(':x1', $x1);
$stmt->bindParam(':y1', $y1);
$stmt->bindParam(':x2', $x2);
$stmt->bindParam(':y2', $y2);

$result = $stmt->execute();

if ($result == FALSE) {
    $info = $stmt->errorInfo();
    echo("<p> Error inserting new Region:</p>");
    echo("<p>{$info[2]}</p>");
    exit();
}
else {
    echo("<p>Region successfully inserted </p>");

    // we only check if there is overlapping when the region is inserted

    if ($result1 == FALSE) {
        $info = $stmt1->errorInfo();
        echo("<p>Error while obtaining the other regions of the last study of this patient: {$info[2]}</p>");
        exit();
    }

    $nrows = $stmt1->rowCount();

    // in case of not finding any regions for this patient in his last study or not finding any study
    if ($nrows == 0) {
        echo("<p>There aren't regions associated with the patient's last study</p>");
    }

    else{

        //checking if x1>y1 and x2>y2, if this condition is not met we change the coordinates
        if($x1 > $x2) {
            $aux = $x1;
            $x1 = $x2;
            $x2 = $aux;
        }

        if($y1 > $y2) {
            $aux = $y1;
            $y1 = $y2;
            $y2 = $aux;
        }

        $flag_overlap = 0;

        foreach($stmt1 as $row){

            //checking if x1>y1 and x2>y2, if this condition is not met we change the coordinates
            if($row['x1'] > $row['x2']){
                $aux = $row['x1'];
                $row['x1'] = $row['x2'];
                $row['x2'] = $aux;
            }

            if($row['y1'] > $row['y2']){
                $aux = $row['y1'];
                $row['y1'] = $row['y2'];
                $row['y2'] = $aux;
            }

            if($x1 >= $row['x2'] or $x2 <= $row['x1'] or $y1 >= $row['y2'] or $y2 <= $row['y1']) { //there is no overlapping for this region
                continue; //next region if exists
            } else {
                $flag_overlap = 1;
                break; //first overlapping, no need to continue
            }
        }

        // if we got to the end and there was no overlap, then we print that message
        if($flag_overlap == 0) {
            echo("<p>There is new clinical evidence for this patient </p>");
        }
    }
}

```

```
    }  
    else {  
        echo("<p>No new clinical evidence - the region inserted overlaps at least with one of the regions of the last study of the patient </p>");  
    }  
}  
}
```

FALTA METER IMAGEM temos que por um screenshot para cada caso???