



# **?id=HIPAA\_violation:**

*exploiting MediatConnect*

Margaret Gorguissian

# What is MedicatConnect?



EHR (Electronic Health Record) software for educational institutions

Allows for messaging between on-campus healthcare providers and clients

Stores immunization records, insurance info, and healthcare invoices

**MedicatConnect serves over 440 colleges and protects the data of more than 4.25 million students.**

# *It does* **protect the** **data, right?** **MedicatConnect lauds** **the security of its** **software.**

As it should, since it's  
dealing with highly  
sensitive information.

## College Health EHR with Type 2 SOC 2 + HITRUST CSF

To ensure storage, handling, and protection of clients' electronic Patient Health Information (ePHI), **meets and exceeds all government and industry standards**. Medicat has made significant investments in its infrastructure and security framework. To substantiate that investment, Medicat has gone through the same third-party audit process as leading data centers in the country and has received Type 1 SOC 2 + HITRUST CSF, and Type 2 SOC 2 + HITRUST CSF Examinations.

A company that has performed Type 2 SOC 2 Examination has proven its system **is designed to keep clients' sensitive data secure over time.** When it comes to the cloud and related IT services, such performance and reliability are essential and required more often by regulators, examiners, and auditors.

"When asked if they are HIPAA compliant, EHR vendors may answer yes. But the only way to prove compliance is for the vendor to successfully complete an external audit, preferably one conducted by a reputable audit firm with HIPAA experience," said Jon Cox, Medicat COO. "The rigorous requirements of a Type 2 SOC 2 + HITRUST CSF Examination provide an **unmatchable level of confidence** and security when considering a move to the cloud. It is critical to ensure your EHR partner has achieved external audits to meet these standards."



### Welcome to Tufts University Health and Wellness Patient Portal

This portal is for students of Tufts University Medford/Somerville Campus and the SMFA at Tufts. Please Log On using your [Tufts University User Name and Password](#).

The portal allows you to access/view:

- Pre Entrance Medical History & TB Risk Assessment
- Enter immunizations and upload your records
- Obtain/print immunization records
- Communicate with your provider via Secure Messaging
- Obtain statements of services
- Medical Insurance - enter this information so we may have it on file for you

[Health Service](#) and [Counseling and Mental Health](#) are committed to protecting your personal information. Data that you provide cannot be viewed by anyone else on the Web and is [securely maintained by industry standard](#) SSL (secure socket layer) encryption and decryption technology when needed. We do not share your information with anyone else.

For general inquiries you can [contact us](#) at 617-627-3350.

# Tufts uses MedicatConnect



## Welcome to Tufts University Health and Wellness Patient Portal

This portal is for students of Tufts University Medford/Somerville Campus and the SMFA at Tufts. Please Log On using your [Tufts University User Name and Password](#).

The portal allows you to access/view:

- Pre Entrance Medical History & TB Risk Assessment
- Enter immunizations and upload your records
- Obtain/print immunization records
- Communicate with your provider via Secure Messaging
- Obtain statements of services
- Medical Insurance - enter this information so we may have it on file for you

[Health Service](#) and [Counseling and Mental Health](#) are committed to protecting your personal information. Data that you provide cannot be viewed by anyone else on the Web and is [securely maintained by industry standard](#) SSL (secure socket layer) encryption and decryption technology when needed. We do not share your information with anyone else.

For general inquiries you can [contact us](#) at 617-627-3350.


# We are VERY secure!

# 1.

## **Lesson One:**

SSL is not the be-all, end-all, of security

## Past Statements [View and Download](#)

-  [Friday, May 04, 2018](#)
-  [Friday, May 04, 2018](#)
-  [Friday, April 27, 2018](#)
-  [Wednesday, April 25, 2018](#)
-  [Saturday, April 21, 2018](#)
-  [Friday, April 20, 2018](#)
-  [Friday, April 20, 2018](#)
-  [Wednesday, April 18, 2018](#)
-  [Friday, April 13, 2018](#)
-  [Thursday, April 12, 2018](#)
-  [Wednesday, April 11, 2018](#)
-  [Thursday, April 05, 2018](#)
-  [Tuesday, April 03, 2018](#)

**Here is a list of  
my  
statements  
from Health  
Services**

# Here's the source code

```
<div class="card">
  <h4 class="card-header">
    Past Statements <small>View and Download</small>
  </h4>
  <div class="card-block">
    <div class="row">
      <div id="ctl00_ContentPlaceholder1_divWalkout" class="col-lg-12">

        <div>
           <a href='walkout.aspx?id=434749' target="_blank">Friday, May 04, 2018</a>
        </div>
        <p />

        <div>
           <a href='walkout.aspx?id=434866' target="_blank">Friday, May 04, 2018</a>
        </div>
        <p />

        <div>
           <a href='walkout.aspx?id=434124' target="_blank">Friday, April 27, 2018</a>
        </div>
        <p />

        <div>
           <a href='walkout.aspx?id=433751' target="_blank">Wednesday, April 25, 2018</a>
        </div>
        <p />

        <div>
           <a href='walkout.aspx?id=433328' target="_blank">Saturday, April 21, 2018</a>
        </div>
        <p />

        <div>
           <a href='walkout.aspx?id=433172' target="_blank">Friday, April 20, 2018</a>
        </div>
        <p />

        <div>
           <a href='walkout.aspx?id=433301' target="_blank">Friday, April 20, 2018</a>
        </div>
        <p />

        <div>
           <a href='walkout.aspx?id=432856' target="_blank">Wednesday, April 18, 2018</a>
        </div>
        <p />

        <div>
           <a href='walkout.aspx?id=432605' target="_blank">Friday, April 13, 2018</a>
        </div>
        <p />

      </div>
    </div>
  </div>
</div>
```



# A closer look

```
<a href='walkout.aspx?id=434749' target='_blank'>Friday, May 04, 2018</a>
```

```
<a href='walkout.aspx?id=434866' target='_blank'>Friday, May 04, 2018</a>
```

```
<a href='walkout.aspx?id=434124' target='_blank'>Friday, April 27, 2018</a>
```

```
<a href='walkout.aspx?id=433751' target='_blank'>Wednesday, April 25, 2018</a>
```

```
<a href='walkout.aspx?id=433328' target='_blank'>Saturday, April 21, 2018</a>
```

```
<a href='walkout.aspx?id=433172' target='_blank'>Friday, April 20, 2018</a>
```

```
<a href='walkout.aspx?id=433301' target='_blank'>Friday, April 20, 2018</a>
```

**walkout.aspx?id=NUMBER**

Interesting...

# What can we infer from this code?



## **Medicat uses the ASP.NET framework**

.aspx files contain scripts that are processed on the server, and the resulting HTML is rendered in browser

## **Statements all have IDs**

The ID field is likely used as a parameter when walkout.aspx runs server-side, so the proper fields are populated in the walkout statement

# Wait, what's a walkout statement exactly?

It details what care you received at Health Services or Counseling and Mental Health Services, and how much it costs

Walkout Statement

Ticket Number: [Redacted]

Federal ID: [Redacted]  
NPI: [Redacted]

Address of Health Services or CMHS [Redacted]

Doctor's name [Redacted]

---

**Responsible Party**

Name: Gorguissian, Margaret S.  
Address: [Redacted] My address

**Account**

Name: Gorguissian, Margaret S.

---

**Diagnosis**

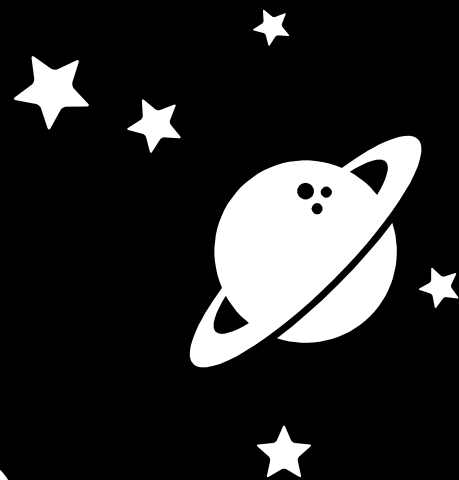
1. [Redacted] My diagnoses

---

Date	CPT Code	Description	Units	Charges
04/27/2018	[Redacted]	[Redacted] A lil more info	1	[Redacted] \$
<b>Total:</b>				

**Today's Balance:**  
Previous Balance:  
Account Balance:

# THIS DATA SHOULD BE PROTECTED



To have it exposed would be a violation  
of HIPAA *and* FERPA



# Spoilers:

It wasn't.



# Exploit Details

- Used 'inspect element' to view source code
- Modified one digit of my walkout statement ID
- Opened link
- It was someone else's walkout statement

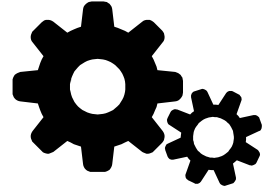
Yes, that was it.

# 2.

## **Lesson Two:**

It is absolutely \*\*\*\*-ing terrifying to find yourself staring at someone else's data.

# Evil Exploit in 3 Easy Steps



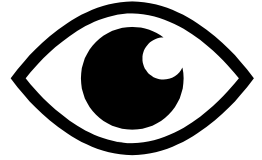
**Script that  
requests pages**

**Generate IDs  
000000  
through  
999999**

**Download all  
statements**



# What are we dealing with?



## Broken Access Control (leading to information exposure)

CWE-284: Improper Access Control

- Access control involves:
  - Authentication (proving the identity of an actor)
  - Authorization (ensuring that a given actor can access a resource)
  - Accountability (tracking of activities) (source: [cwe.mitre.org](https://cwe.mitre.org))
  - Medicat failed on authentication and authorization, and *maybe* accountability

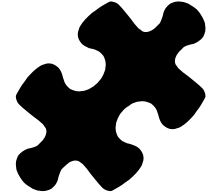
CWE-639: Authorization Bypass Through User-Controlled Keys

- User can access another user's data by modifying the access keys



# The Response

- Reached out to Ming immediately, who forwarded it to Lorna (Tufts Information Security)
- The next day, Megan & Donna (from the CS Main Office) pushed us to contact Tufts General Counsel
- They reached out to Medicat, who fixed it in <1 week



# The Fix

- If you try to access an ID you should not have access to, you get auto-logged out
- Medicat says this vulnerability was never leveraged according to their logs
  - But how strong do we know their *accountability* is?

# Final Thoughts

## **It's super easy to be cynical about this**

Medicat boasts about their security and their certs, but failed on basic access control. What other systems are like this? (*lots*)

## **Basic access control is a constant issue**

It consistently makes the OWASP Top 10.

## **(I think) People want to fix things**

I was very pleased that Tufts Legal Counsel, Tufts Information Security, Tufts Health Services, and Medicat rapidly took the steps needed to fix things.

## **Having allies & mentors make all the difference**

Thanks Ming!