**Seminar 2 Preparation**

STRIDE is an acronym for the types of threats it covers, which are:

* **Spoofing**—a user or program pretends to be another
* **Tampering**—attackers modify components or code
* **Repudiation**—threat events are not logged or monitored
* **Information disclosure**—data is leaked or expose
* **Denial of service (DoS)**—services or components are overloaded with traffic to prevent legitimate use
* **Privilege escalation**—attackers grant themselves additional privileges to gain greater control over a system

In Healthcare industry, I found that the below cases were more commonly used.

**Spoofing**

UPHS-Marquette: Hospital’s number being used through ‘caller ID spoofing’

<https://www.uppermichiganssource.com/2021/03/18/uphs-marquette-hospitals-number-being-used-through-caller-id-spoofing/>

**Information disclosure**

Healthcare Data Breach Statistics

<https://www.hipaajournal.com/healthcare-data-breach-statistics/>

Disclosing patients' personal information: a framework

<https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/disclosing-patients-personal-information-a-framework>

**Denial of service (DoS)**

Hospitals worldwide hit by wave of cyberattacks seeking to crash websites during Covid-19 pandemic, report says

<https://www.standard.co.uk/tech/hospitals-hit-by-wave-of-pandemic-cyberattacks-a4516206.html>