**Report : Health Data Protection and Privacy**

**Motivation:**

**Why did you choose your topic(s)?**

Data related to health is always sensitive and there have been many laws framed around the protection of public health information like The Health Insurance Portability and Accountability Act of 1996 (HIPAA) that mandates the development of national standards to guard against the disclosure of sensitive patient health information without the patient's knowledge or consent. By 2009, more than 40 % of the Hospital groups have adopted full or partial Electronic Health Record(EHR) Systems. However due to the increase in the use of digital technologies in health care like IoT devices which constantly collects the data like heart rate, sleeping habits, and physical activities. Even booking an appointment for a doctor consultation is becoming online. With all the exposure to health data online and companies trying to trade data for their benefits, there will be a potential harm to users. So, I have picked a topic involving the risk of public health information and how it can be misused.

**Issues:**

**What are the potential harms involved with your topic?**

Article 17 of the ICCPR (International Covenant on Civil and Political Rights) protects everyone from arbitrary or unlawful interferences with their “privacy, family, home, or correspondence”. Health organizations are exploiting the data of users for their benefit. There have been several threats involving public health data by how the health care organizations collect, store, and interpret the data. Following consequences might lead if public health information is traded.

**1)Pregnancy/Abortion Details :**

Most women want to keep their pregnancy status private however Recent article in markup on a company called Hey Jane an online abortion pill vendor making the customer's details available to Facebook pixel ad tracker and other third-party online sites states that the user's information is not secured.

**2)Sexual Orientation :**

Most people tend to keep their sexual orientation private whereas the diagnostic companies trading in this kind of test reports result in the exposure of the sexual orientation of the respective person. It may cause severe anxiety problems and mental health issues in people if their information is traded online and if hackers get the data, they might blackmail the concerned people.

**3)Bank Details :**

The user data if containing payment details of some users when traded by health organizations might cause a potential risk to users as it might lead to cyber fraud.

**4)Contact and Location Information :**

The user data containing contact and address information when traded by health organizations exposes the locality of users and their identity. Recently a popular safety app Life360 has sold precise locations of its tens and Millions of Users.

**5) Children's Health Data :**

Children's health data is precious as children tend to be less immune to diseases. Access to children's health information can be an advantage to Hospitals and Medical agencies may target the parents of the children for consultation with them and subscribe to their products for immunity boosting. Recently Children’s Hospital group Nemour has shared the children's health records with Facebook.

**6)Health Reports :**

Health Reports can be used by companies to target marketing their medical products.

**7)Insurance Information :**

Your Insurance details can be used in a variety of ways, including making claims with your insurance company, purchasing medical devices, receiving medicines, visiting a doctor, and more.

**Stake Holders:**

**Who is or could be harmed:**

**General Public :**

The general public would be potentially at risk if their medical information is traded online and made available as companies use the details for their benefit rather than the benefit of the user. For instance, the company having access to the medical information of a person might market the relevant medical devices and medicines.

**Children :**

Children are often sensitive and they are mentally not that stable to interpret the data they see. Companies having the Children’s health details might show them an ad relevant to the disease they are suffering with. If the child clicks the ad and gets the consequences of the disease he is suffering with might end up creating more fear in the child.

**Health Workers :**

Often big tech companies and health organizations end up messing up with user health data privacy and hitting up the headlines which creates a false image of doctors and nurses in people.

**Who is involved in the potential harm:**

**Big tech companies/Social media companies:**

The greed for competitive advantage is true and companies are exploiting user-related data mostly for targeting ads. Even with the development of technologies like AI/ML, companies need huge amounts of data to train their models for predictive analysis. Moreover, companies are trading public health information data with health firms.

**Hospitals:**

Hospitals are benefitting greatly by trading user data with big tech companies. Most of the hospital websites are having web tracking tools for users like Facebook pixel which in turn collects user activities and uses the data for Facebook advertising.

**Health Insurance Companies and Pharmaceutical firms:**

Health Insurance Companies are benefitting by subscribing to targeting ad campaigns run by some tech companies.

**Hackers:**

Hackers tend to collect personal information of people online via unsecured sites which might have got data from health organizations and misuse personal information.

**What could be done with FTC regulation**

**1)[Data Collection and us](https://www.cdc.gov/nchhstp/programintegration/sc-standards.htm" \l "DATA" \t "_blank)e process**

**Who would be required to implement/change?**

Health organizations should be transparent and let the users know how their data can be interpreted. They should collect minimal user information and should prefer to collect non Identifiable data whenever possible. Companies should more over take consent from the users to involve their data in any scientific studies.

**Who would benefit?**

The users of the Hospital would benefit from this as it won’t affect their privacy if proper data collection and using techniques are employed by health organizations.

**Role of Computer scientists/software engineers?**

Computer scientists should come up with techniques that can process minimal information efficiently as we know we need huge datasets for predictive analysis.

**Pros/Cons**

Pros:

User data would be protected.

One’s identity on the internet is kept private.

Minimal information about a user is collected.

Data is used properly.

Cons:

Minimal user data won’t be good to make observations and scientific experiments.

**2)Data Sharing and Release**

**Who would be required to implement/change?**

Health Organizations should not trade or share data with their partner companies without abiding by the data laws and if it’s for a reasonable purpose they should take consent from users and make sure that the data is not misused by their partner companies. Health-related data gathered by smart devices should be kept private. Moreover, companies using cloud services should make strict terms related to data privacy while working with cloud providers.

**Who would benefit?**

The users of the Hospital would benefit from this as it won’t affect their privacy if proper data collection and using techniques are employed by health organizations.

**Role of Computer scientists/software engineers?**

Computer scientists should come up with techniques that make sure the data will be transferred securely between the organizations and their partner's systems.

**Pros/Cons**

Pros:

Health Data trading won’t happen.

Our data will be secured as it is not made visible to all companies.

Unwanted spam calls or ads from other companies can be reduced.

Cons:

Not sharing important data with a partner company might result in bad terms between organizations.

**3)Data Security**

**Who would be required to implement/change?**

Organizations should implement advanced encryption standards on user data and should make sure that data breaches should not happen on the company's database.

**Who would benefit?**

Data breaching has been gradually increasing, and maintaining robust security standards by organizations will benefit users.

**Role of Computer scientists/software engineers?**

Computer scientists should come up with advanced hashing or encrypting techniques employed to user data to protect their identity.

**Pros/Cons**

Pros:

Data Breaches won’t happen easily in health systems.

Cons:

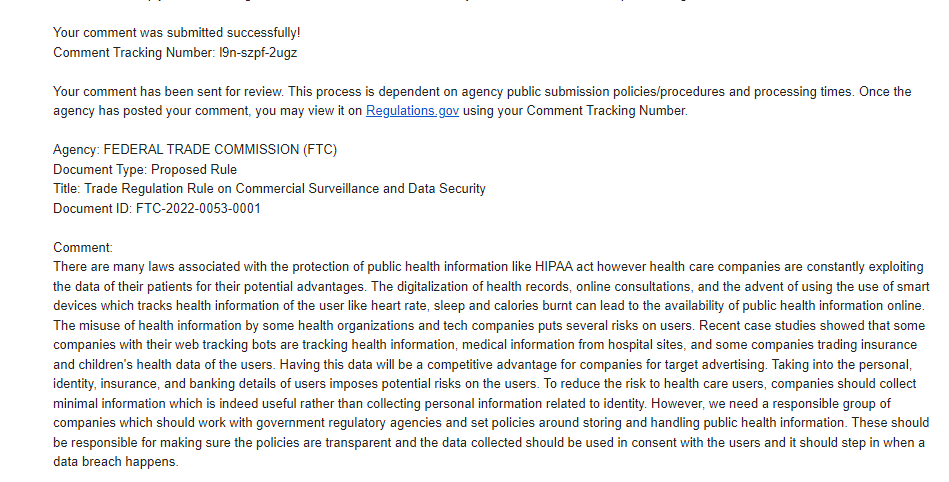
More complexity in hashing or encryption needs high computer resources.

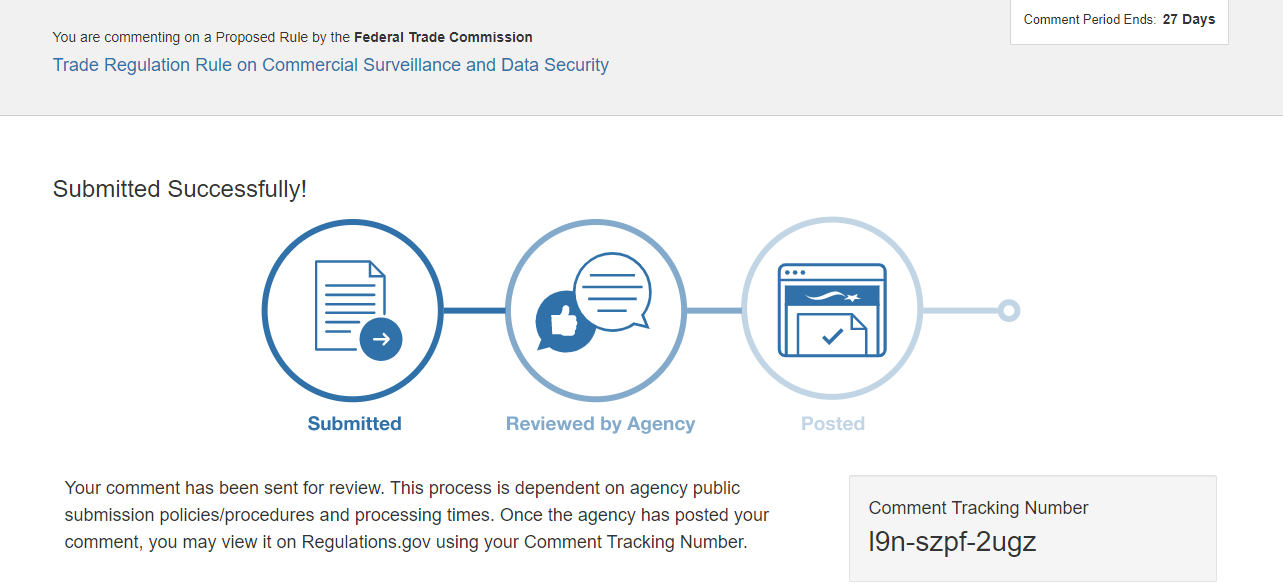
**Recommendation for regulation:**

**What approach do you recommend?**

I would recommend that health companies should set up responsible teams which should work with government agencies and set up policies around data. Moreover, they should be responsible in the organization to check whether all data policies in place are being executed. This team should investigate immediately when a data breach happens in a company and make sure they do not occur in the future. These teams should pick up the complaints from the general public when something goes wrong or when their data is leaked and act on them immediately. They should make sure that staff is regularly given training on data security.

**Appendix:**

****

****

**References:**

<https://themarkup.org/pixel-hunt/2022/07/01/online-abortion-pill-provider-hey-jane-used-tracking-tools-that-sent-visitor-data-to-meta-google-and-others>

<https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

<https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook>

<https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user>

<https://bmcbioinformatics.biomedcentral.com/articles/10.1186/1471-2105-12-S12-S7>