

White Paper

CUNIX

Securing PI and PHI: Information Security in Healthcare Sector

Rajendra Pratap Singh



The use of Information Technology with increased digitization, transmission and mining of information has made the Healthcare sector more efficient and cost effective. At the same time, it has also resulted into an increased privacy and security risk related to personal information (PI) and personal health information (PHI).

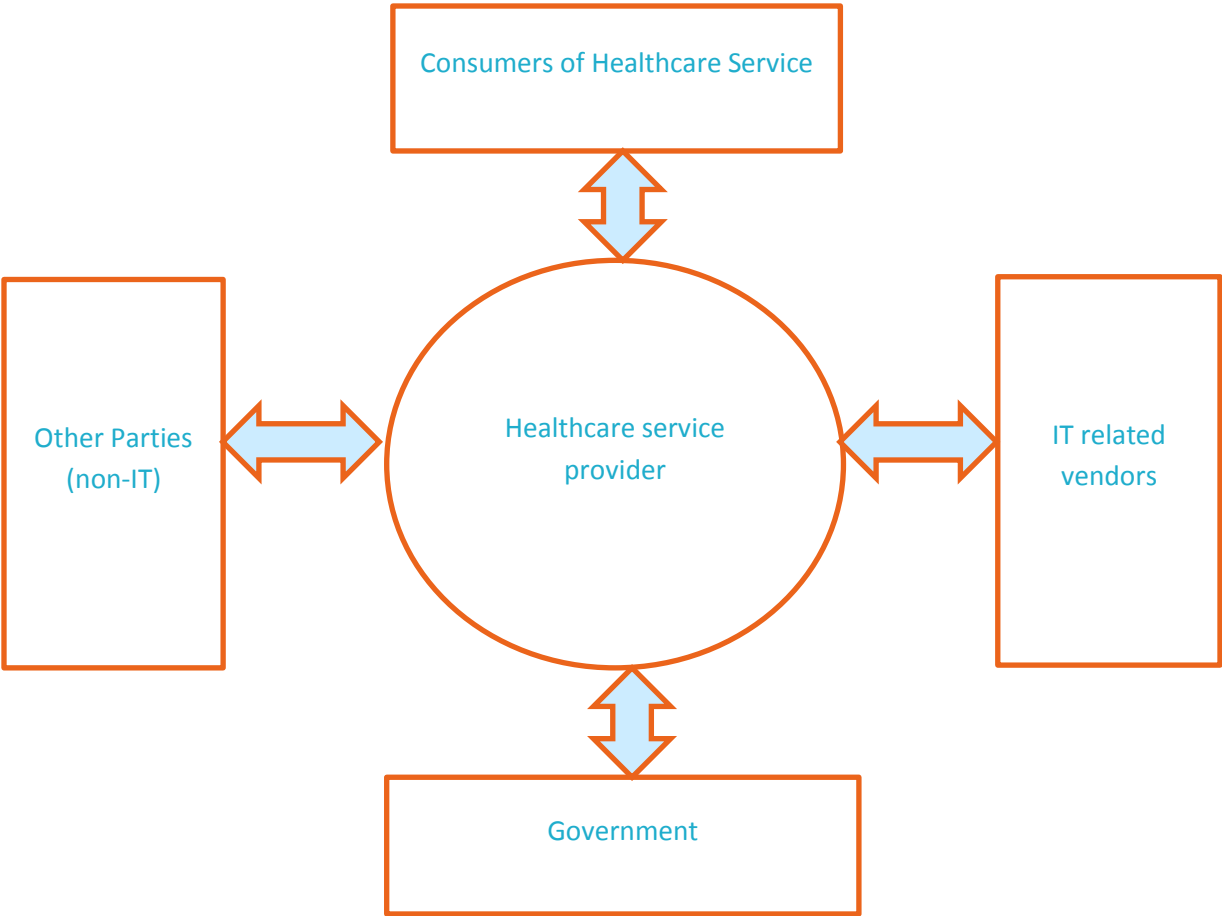
The impact on confidentiality, integrity and availability of health information can have a devastating impact on the patient's health and even life.

Overview

If we analyze the Healthcare sector ecosystem, the entities are described below:

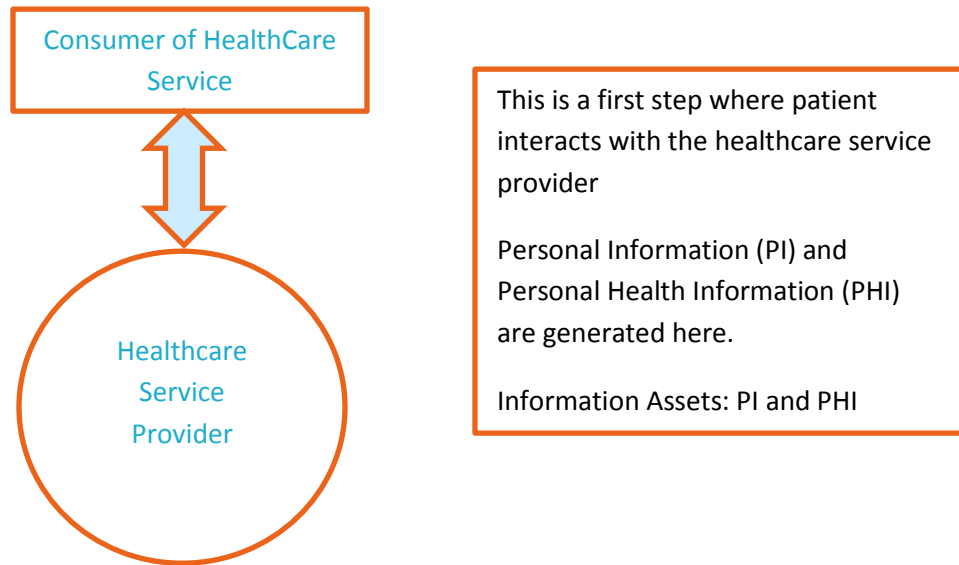
- 1) Healthcare service provider
- 2) Consumers of Healthcare service
- 3) IT related vendors to Healthcare service provider
- 4) Other vendors to Healthcare service provider
- 5) Government

In this ecosystem, whenever these entities interact there is sharing of information. Healthcare service provider also shares the information internally. All these transactions between all these entities lead to potential information security concern and threat of information theft leading to social and monetary impact.

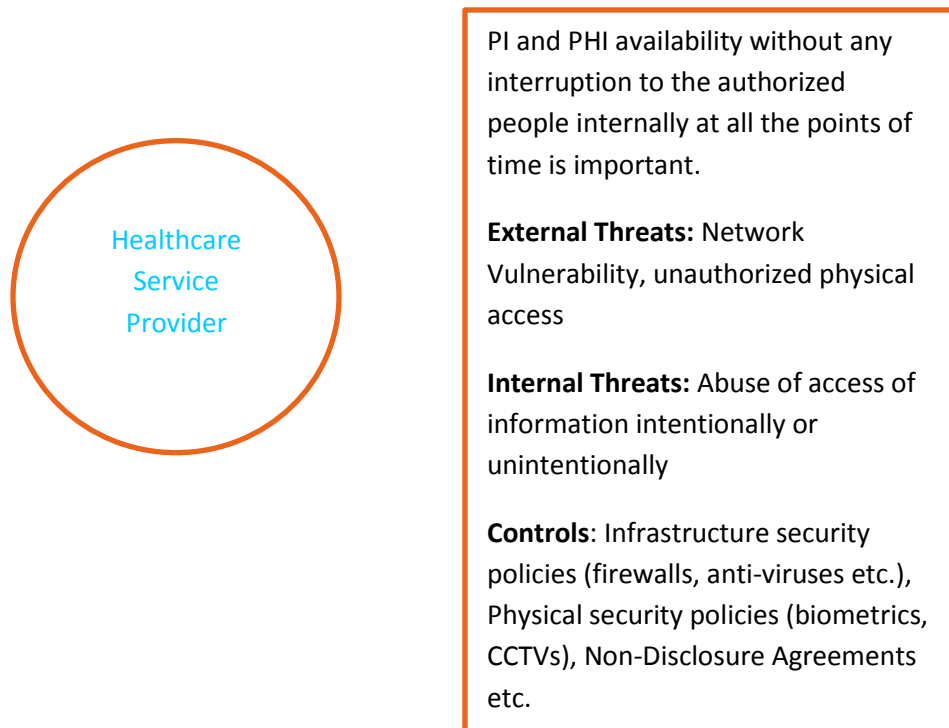


What these entities share during their interaction?

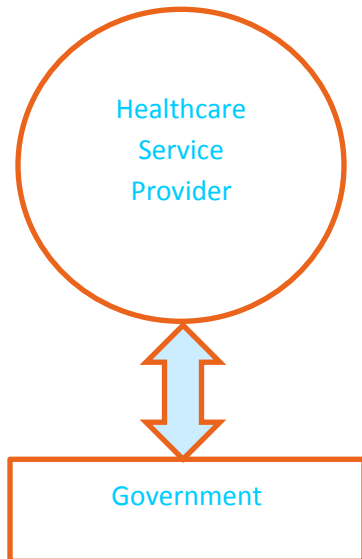
1) Healthcare service consumers and healthcare service providers:



2) Interaction inside the Healthcare service provider organization:



3) Healthcare service providers and Government:



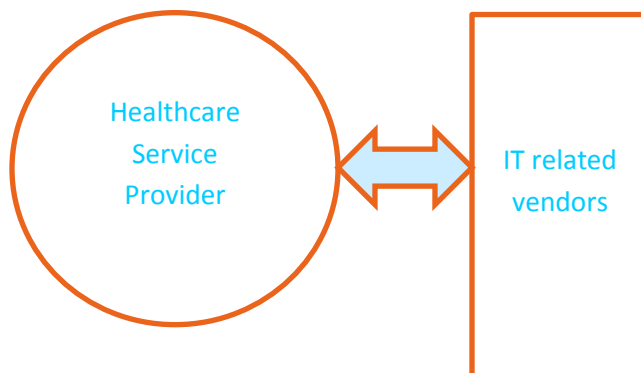
There is a frequent interaction between the Healthcare service provider and the Government.

Government needs information to devise and run the social well-being policies for senior citizens and poor.

Threats: Leakage of information during the transfer, mishandling of data at government's end

Controls: Third party agreement

4) Healthcare service providers and IT related vendors:

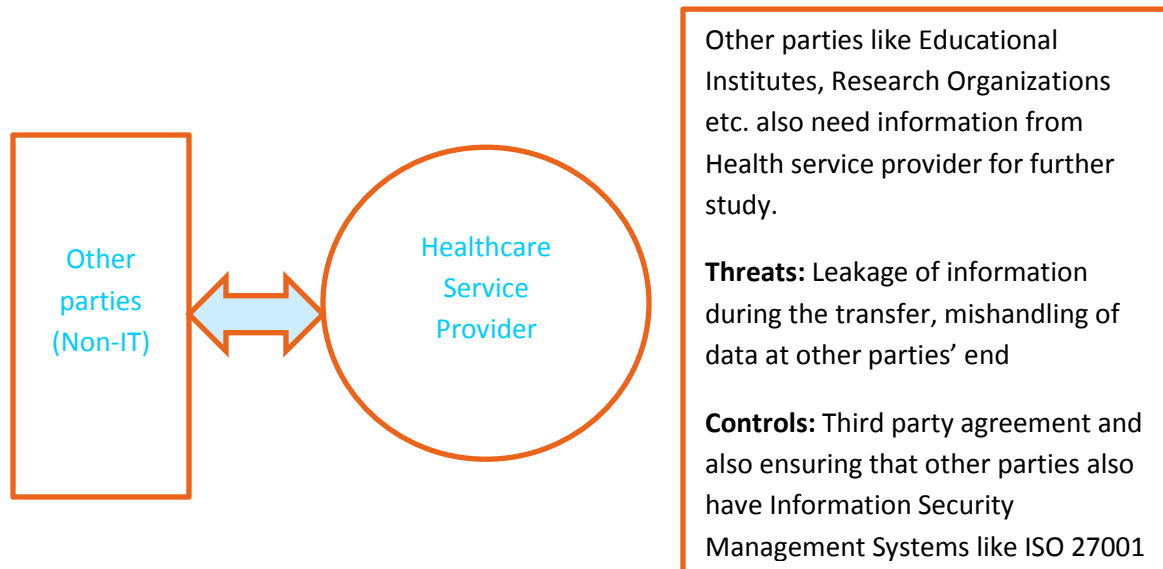


There is a real time interaction between IT vendors and Healthcare service providers for Back-up and Storage, Billings, Analysis etc.

Threats: Leakage of information during the transfer, mishandling of data at IT vendor's end

Controls: Third party agreement and ensuring that IT vendor also has Information Security Management Systems like ISO 27001

5) Healthcare service providers and Non-IT related parties:



Personal information and personal health information are important information assets for the healthcare service provider. Protection of these assets is important for reputational and monetary benefit of the Healthcare service provider.

There are many more information assets presents in the organization. The threats, vulnerabilities and controls differ according to the context.

CUNIX is CMMI Institute Partner for CMMI Appraisals. CUNIX consults in area of GRC (COBIT, COSO, HIPAA, ISO 27001, ISO 20000, SOX, ISO 31000, and ISO 22301), IT Process Improvement, Balanced Score Card, Business Excellence, Operational Effectiveness, QPO, Six-Sigma, Management Systems etc.

Contact CUNIX: business@cunixinfotech.com