

Health & Right to Information – newer paradigms

DR SABAHAZ AZIM
MD & CEO, GLOCAL HEALTHCARE SYSTEMS

Introduction

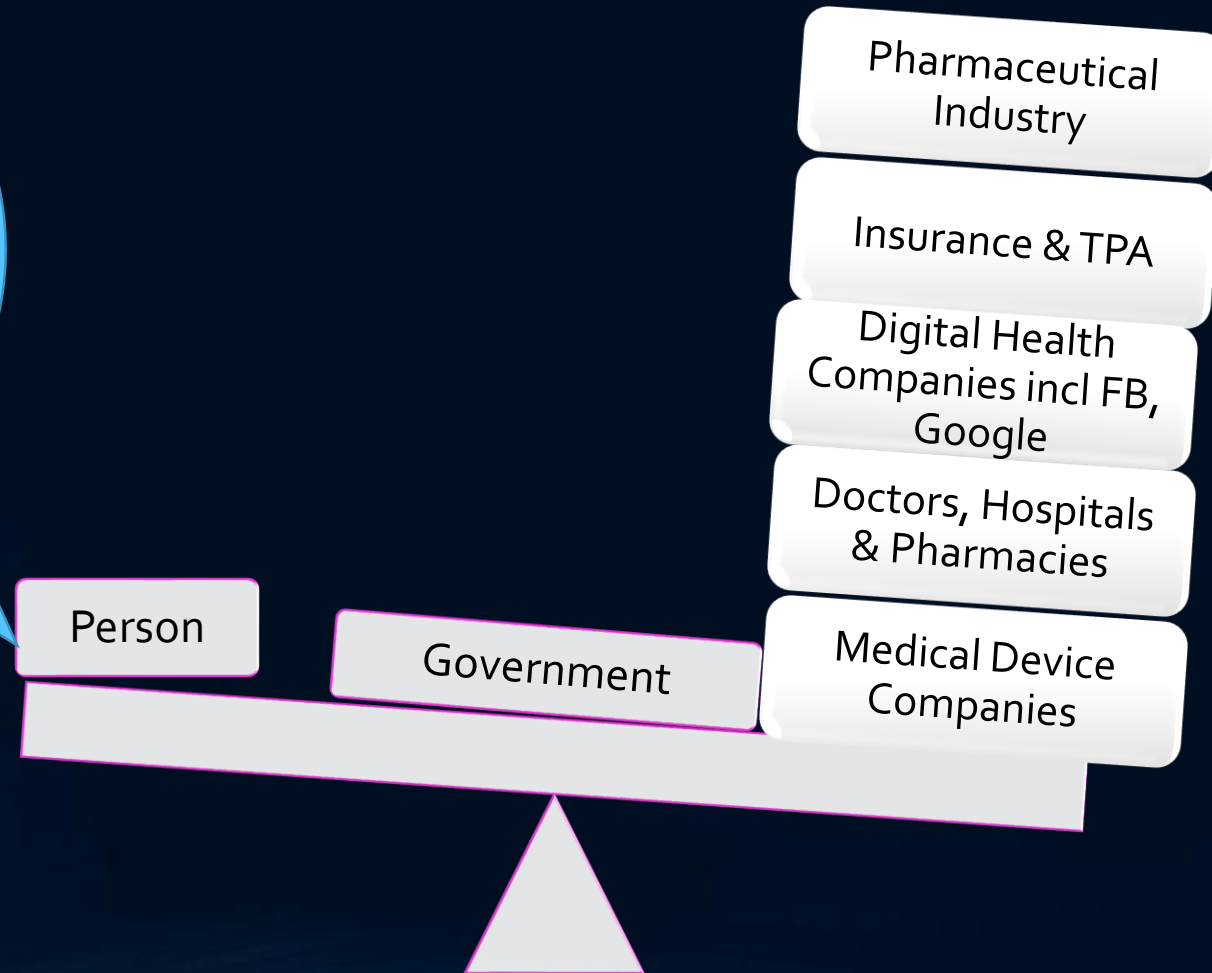
- The interplay of right to Information & health has generally been seen as a legal issue
- This presentation wants to focus on a perennial problem of who owns the medical data especially in light of emerging digital world
- This is just one perspective and represents personal views of the author and do not represent the views of the organization

Health Information Stake Holders



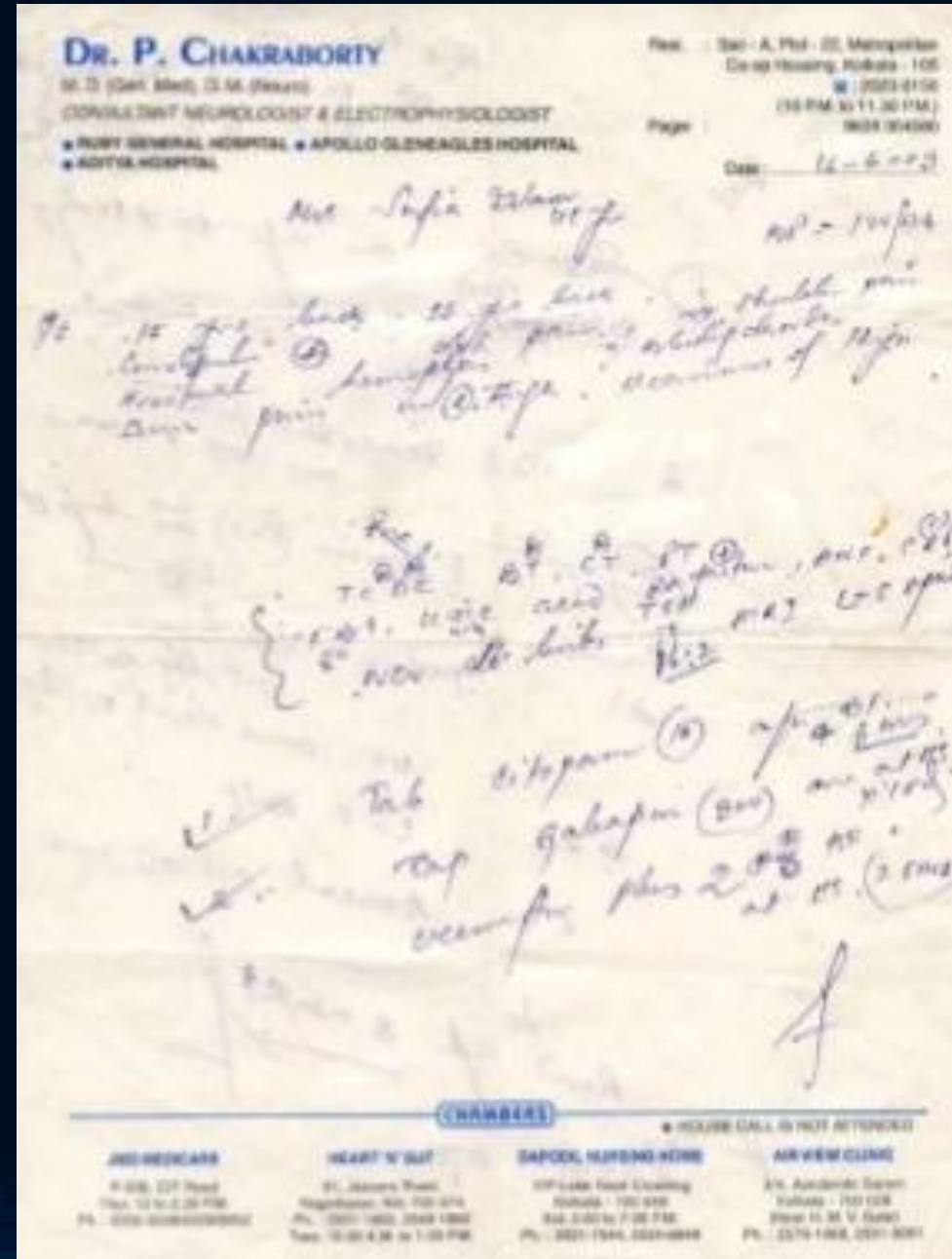
Health Information Power Play

Least Power over own
medical data



Information Poverty of Patients

- Medical Knowledge Asymmetry
- Jargon
- Lack of consent
- Illegible & incomplete Prescriptions
- Discharge Certificate instead of medical record
- Privacy protection incomplete & cost of exercising the protections



Most medical data of a person lies with others

- Insurance companies need data - they say - to process claims
- Doctors & HCOs need data – they say – to provide healthcare
- Pharmaceutical companies acquire data in bulk – they say – to research
- Government needs data – it says – to protect people
- Today, digital entities including Facebook, Google, wearables, medical device companies including implant & software companies acquire data for research & development to deliver “better content”
- But most data is used commercially without the data owners consent

Basic Principles

- Your medical & wellness data belongs to you and is a 'privileged communication' irrespective of whether you paid for the health service or the government or your employer paid for you. A person has the right to privacy.
- Only if public interest has to be protected, data should be shared e.g. an epidemic or a notified disease, does it need to be communicated. It should be done in such a way as to protect the privacy of a patient.
- All other uses including for research, actuarial, claim processing, customization of services should be treated as clinical research & an ethics committee should approve the data acquisition activity and then informed consent needs to be taken. Implied consent in the form of usage of a service and hidden click wrap agreements need to be banned,

The Difficulty of being Good

- HIPAA, CEA, Multiple & inconsistent laws, legal trigger happy authorities, business hungry entities, investors demanding high returns, customers in need of medical services or products make this Gordian knot tough but exciting to unravel.
- No easy answers to what needs to be protected. Where does the freedom to wave your hand ends and where does someone else's nose begin is a tough question to answer.
- Legal solutions are slow, bring more confusion and will always be behind times.

Technology alone can solve problems of technology

FROM BIG DATA TO ZERO DATA : COMBINING BLOCKCHAIN WITH ZKP TO
CREATE RIGHT OF INFORMATION IN HEALTH WITHOUT STOPPING WORK

Block Chain

A **blockchain**, originally **block chain**, is a continuously growing list of records, called *blocks*, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority (from Wikipedia)

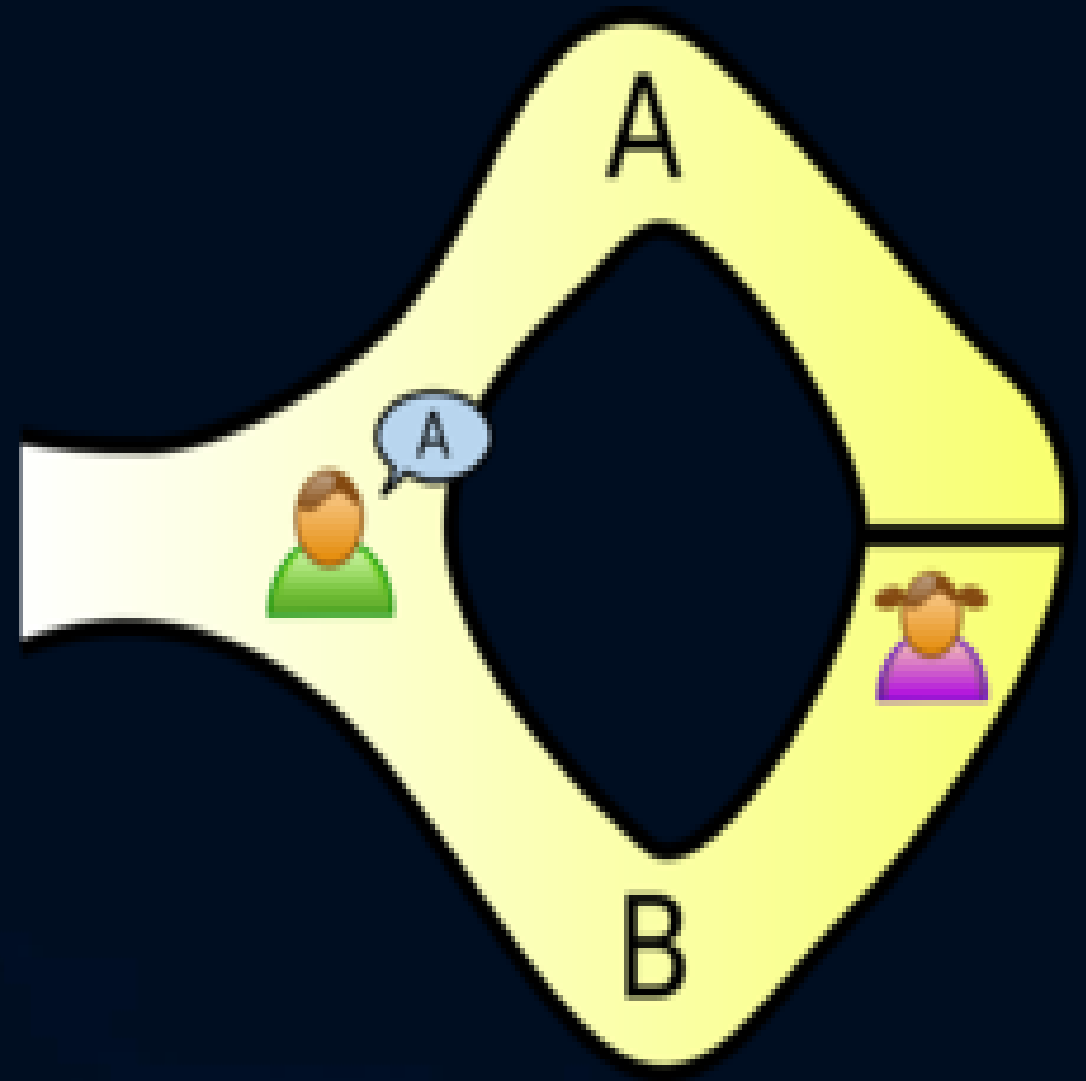


Zero Knowledge Proof

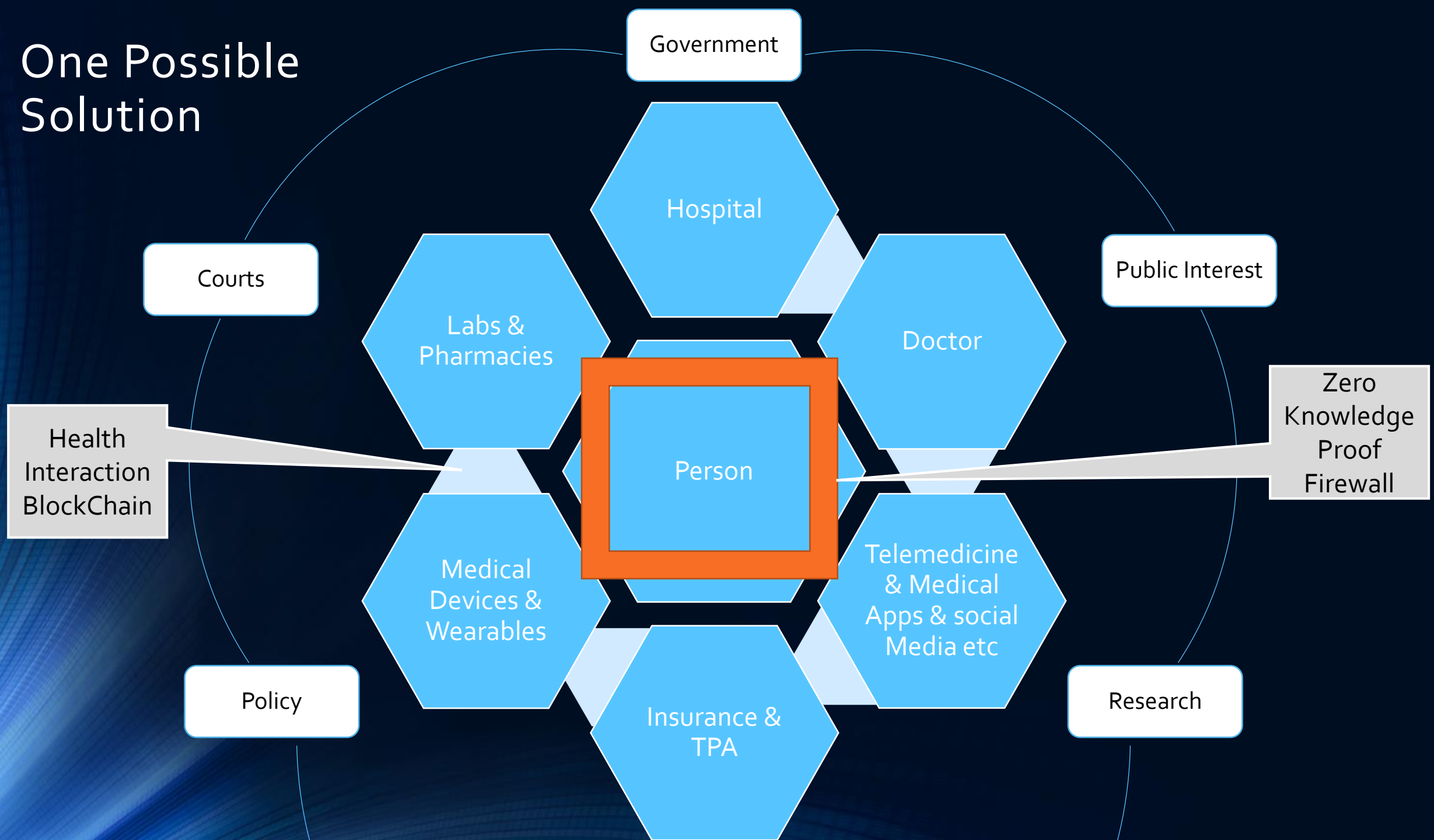
In cryptography, a **zero-knowledge proof** or **zero-knowledge protocol** is a method by which one party (the *prover* Peggy) can prove to another party (the *verifier* Victor) that she knows a value x , without conveying any information apart from the fact that she knows the value x .

Another way of understanding this would be: Interactive zero-knowledge proofs require interaction between the individual (or computer system) proving their knowledge and the individual validating the proof.

If proving the statement requires knowledge of some secret information on the part of the prover, the definition implies that the verifier will not be able to prove the statement in turn to anyone else, since the verifier does not possess the secret information. Notice that the statement being proved must include the assertion that the prover has such knowledge (otherwise, the statement would not be proved in zero-knowledge, since at the end of the protocol the verifier would gain the additional information that the prover has knowledge of the required secret information). If the statement consists *only* of the fact that the prover possesses the secret information, it is a special case known as *zero-knowledge proof of knowledge*, and it nicely illustrates the essence of the notion of zero-knowledge proofs: proving that one has knowledge of certain information is trivial if one is allowed to simply reveal that information; the challenge is proving that one has such knowledge without revealing the secret information or anything else.



One Possible Solution



Right to Information must protect the individual

“GIVE TO CAESAR WHAT BELONGS TO CAESAR; GIVE TO GOD
WHAT BELONGS TO GOD BUT FIRST GIVE TO THE INDIVIDUAL
WHAT BELONGS TO HIM”



Glocal Healthcare Systems
11 Hospitals, 253 Digital Dispensaries,
Online Virtual OPD, Medical Apps &
more ...

Dr Sabahat S Azim
Glocal Healthcare Systems
3B 207 Ecospace, New Town Kolkata
700156

ceo@glocal.healthcare

+91-33-66081000

Thank You