Information and technology law course

LECTURE 21 – 2 DECEMBER 2024

FEDERICA CASAROSA – 2024/2025

Cloud computing

Way to share availability of data, application etc. Different actors: providers of cloud, or even owner of cloud etc. Generally used for IaaS, You don't need infrastructure, you can rent it somewhere.

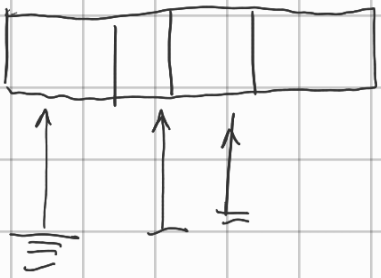
Unavailability is completed with cloud computing

Definition technical

organization providing standards at US level

According to National Institute of Standards and Technology (NIST) a 'computing capacity' will qualify as a 'cloud service' if it has the following five characteristics:

1. 'on- demand self- service' → 1. I can decide what type of capabilities I need on demand, without need of additional service
2. 'broad network access' (offers) → 2. Using internet, usable through different types of devices
3. 'resource pooling' (has)
4. 'rapid elasticity' and
5. 'measured service'. → 3. Computer resources can be pooled to multiple users: multi-tenant model ⇒ more than 1 subject using the same structure. Virtual and Physical resources are assigned based on demand



What if one doesn't need it anymore? I can reorganise the provision of resources.

This is connected with RAPID ELASTICITY

⑤ Connected also to other 2: cloud sys can automatically control and optimise resources.

Models of Cloud services

Infrastructure as a Service

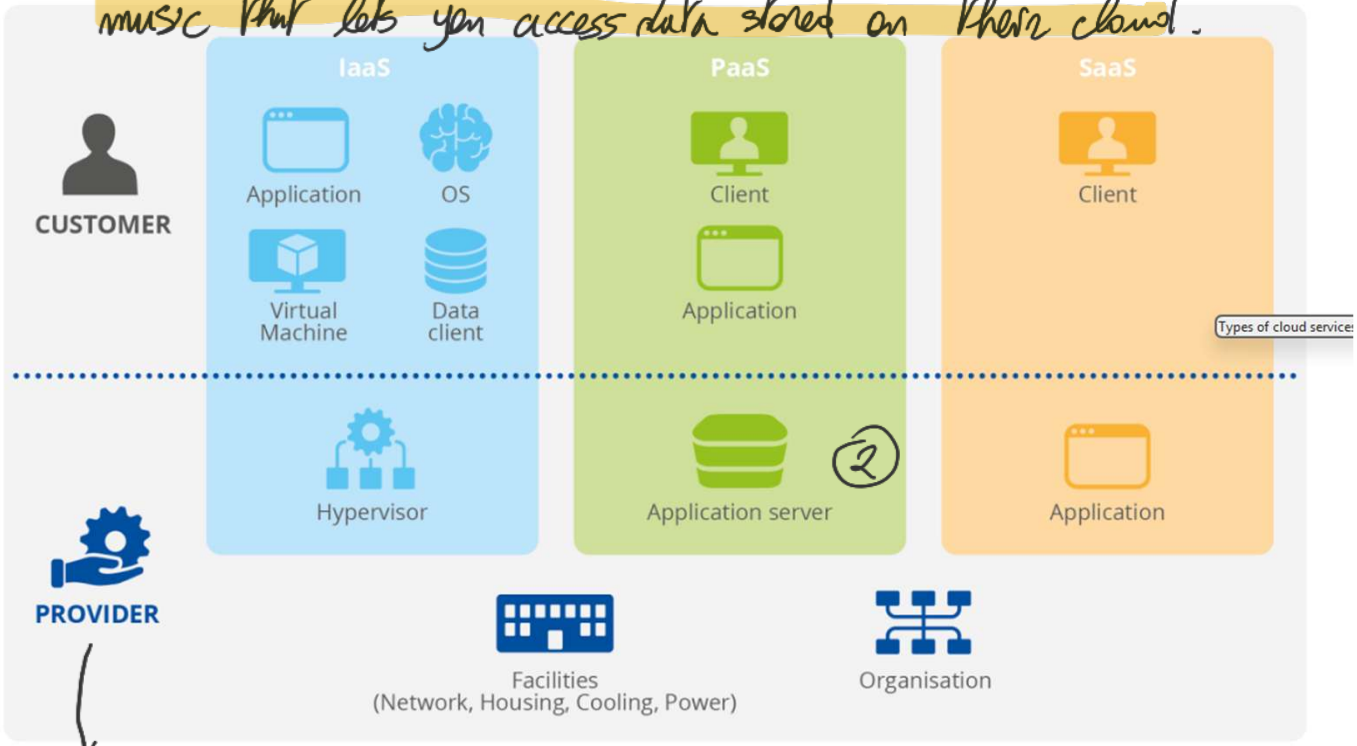
Platform as a Service

Software as a Service

By ENISA: Infrastructure aaS:

PaaS:

SaaS: easiest/most used: software on demand. Spotify. YT vs streaming music that lets you access data stored on their cloud.



Provider has the application and then you have the client application downloadable by customer.

Also for businesses: Unwipu works with Teams, so we have public and private actor.

② Here you have application and the server: imagine Word on dropbox, have the application online to deal with the server.

① Physical machines, VM, networking, storage. Customer has more options that can be chosen. Not easy to distinguish IaaS and PaaS: ex. you have your company website and you want it on the cloud, IaaS can be the host. Then you might want add-ons and that could make the provider provide PaaS too.

What is PaaS?

PaaS is a cloud service model that provides a complete environment for developers to build, run, and deploy applications. Unlike IaaS, where you manage the infrastructure, PaaS takes care of everything below your application. This means you don't worry about setting up servers, operating systems, or middleware.

You only focus on your **application code and data**.

What Does PaaS Provide?

1. **Development Tools:** Tools for coding, debugging, and testing applications.
2. **Runtime Environment:** A ready-to-use environment where your app can run (e.g., Java, Python, Node.js).
3. **Managed Infrastructure:** The servers, storage, and networking are handled by the provider.
4. **Built-in Scalability:** Your app can scale automatically based on demand without you configuring servers.
5. **Database and Middleware:** Pre-configured services like databases (e.g., PostgreSQL) and middleware (e.g., message queues).

IaaS (Infrastructure as a Service):

This is the most basic level. It provides the *barebones* resources like virtual machines, storage, and networking. It's like renting a computer in the cloud where you control almost everything, including the operating system, apps, and configurations. You handle the setup and maintenance of the software yourself.

Example: If you were building a house, IaaS would be like renting a plot of land and getting raw materials (bricks, cement, etc.). You have to build the house yourself.

- **Popular providers:** AWS EC2, Google Compute Engine, Microsoft Azure Virtual Machines.

Types of cloud services

Private cloud: Spolwfy: anybody can access but for subscriptive = close system, only

single org. have their own internal cloud

Community cloud = specific community of consumers: operated by possibly a certain # of org.

Public cloud = open to the general public

Hybrid cloud = between public and private

Cloud service levels

- the **data level**, representing the data household of cloud computing, with both stored data and data in transit;
- the **application level**, representing installed applications using the cloud computing resources (hardware and software);
- the **network level**, representing the network elements/service used by the cloud computing node, including security elements responsible for the network protection;
- the **host level**, representing all elements supporting the virtualisation functions, such as the virtual server, virtual machines and the hypervisor.

1. Data Level

- This level focuses on the **data** itself, including both **stored data** (e.g., files, databases) and **data in transit** (e.g., data being transmitted over the network).
- It's responsible for managing, securing, and processing information within the cloud.
- **Key concerns:** Data encryption, privacy, and ensuring secure communication (e.g., using HTTPS or VPNs).
- **Example:** Your files on Google Drive or messages being sent through a secure cloud application.

2. Application Level

- This refers to the **software and applications** running in the cloud, utilizing both hardware and software resources.
- These applications can include tools like email platforms (Gmail), customer relationship management systems (Salesforce), or development tools.
- **Key concerns:** Ensuring the reliability, availability, and performance of the applications.
- **Example:** When you use Google Docs, the application level manages the editing and saving of documents.

3. Network Level

- This level deals with the **network infrastructure** that connects cloud resources. It includes routers, switches, and security services like firewalls.
- It's responsible for managing **network traffic**, ensuring secure connections, and protecting the system from cyber threats.
- **Key concerns:** Bandwidth, latency, and network security (e.g., DDoS protection).
- **Example:** When accessing a cloud-based app from your browser, this level ensures data is transmitted securely and efficiently.

4. Host Level

- This level includes the **virtualization infrastructure**, such as virtual machines, servers, and the hypervisor (software that enables virtualization).
- It provides the foundation on which virtual environments are created and managed.
- **Key concerns:** Efficient allocation of physical hardware resources and isolation between virtual machines.
- **Example:** AWS EC2 instances running multiple virtual machines on a single physical server.

EXAMPLE: healthcare cloud

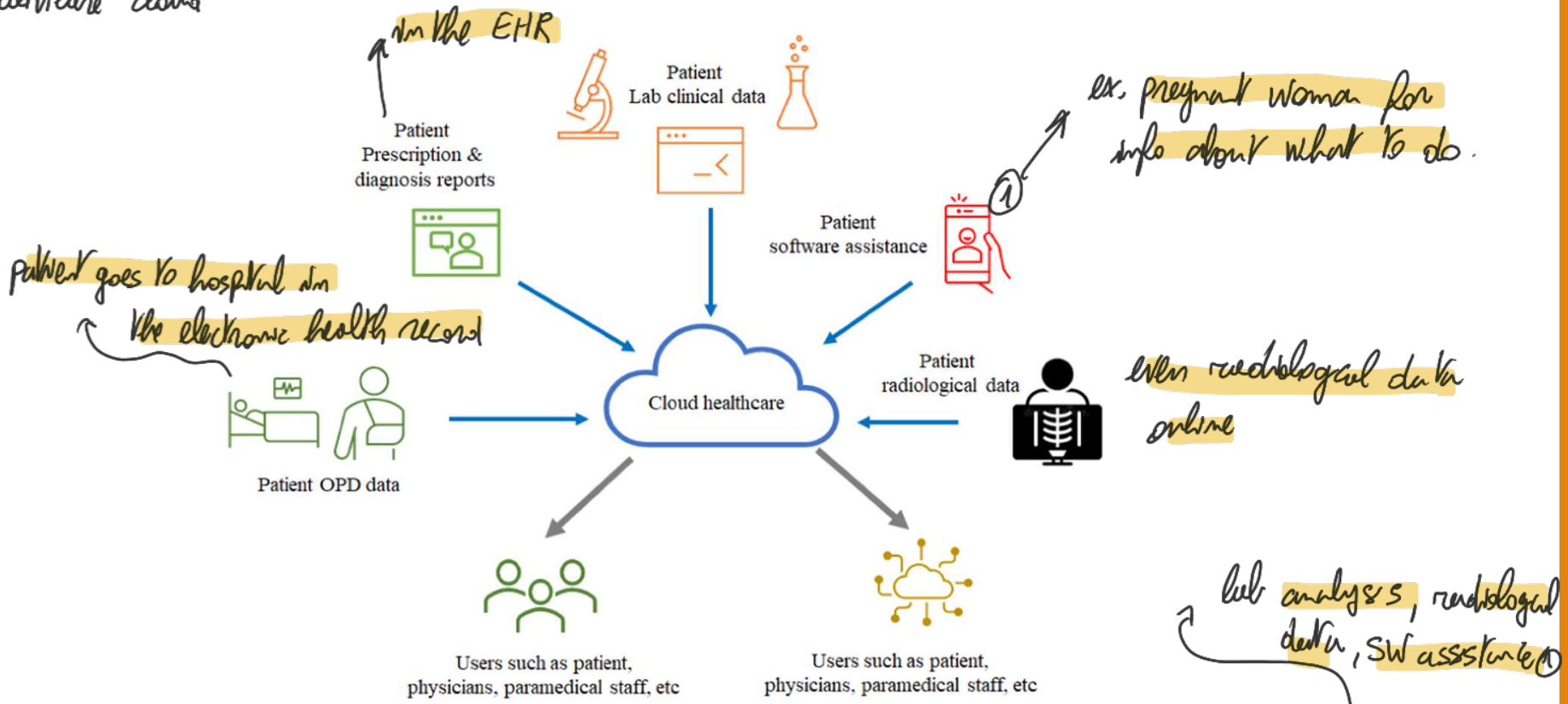


Fig. 4. Typical healthcare cloud.

8

in the EHR

ex. pregnant woman for info about what to do.

patient goes to hospital in the electronic health record

even radiological data online

lab analysis, radiological data, SW assistance

You can also check your electronic health record,

Even blood control for example: you can download lab analysis data online. All is coordinated within ce

cloud. All those elements can be connected because they might be accessed the same cloud sys.

EU health data space: regulat. proposal to create a common EU data space where you can have access to

your EHR throughout Europe.

So, different actors that can be involved.

Cybersecurity in Cloud service

ENISA Cloud Cybersecurity Market Analysis, March 2023 "What is happening at the moment"

"Various gaps in the cloud cybersecurity market emerge through mismatches in deployment of ① cybersecurity functions between the demand side and supply side. The market gaps are rooted in concerns about the management of various threats and unclear distributions responsibilities about the implementation and maintenance of cloud cybersecurity functions."

↳ Recent analysis says that it's not easy to understand who does what in terms of CS.

Stakeholders involved:

- the demand side, which includes the end users of cloud services;
- the supply side, which includes cloud service providers (CSPs) and cloud enablers;
- organisations conducting R & D in cloud computing;
- bodies involved in regulation, covering regulatory activities in could computing.

① Not clear who is in charge of CS measures between who is the provider and the deployer. Should I, as a patient, be the one that adopts security for the overall system? There might be different levels of obligation

Cybersecurity in Cloud service

Relationship between cybersecurity and cloud computing

- Companies in cybersecurity market segments can relate to cloud computing in several ways, such as by providing
  - security from the cloud,
  - security for the cloud computing infrastructure (e.g. secure stack components)
  - security in the cloud (e.g. confidentiality of data in the cloud).

} Connected but obsenvangled.

- Similarly, companies from the cloud computing market segment may offer:
  - public cloud services
  - independent software vendors
  - managed cloud, brokers etc.

③ For example, guarantee confidentiality. Make sure that stored or transiting info is protected.

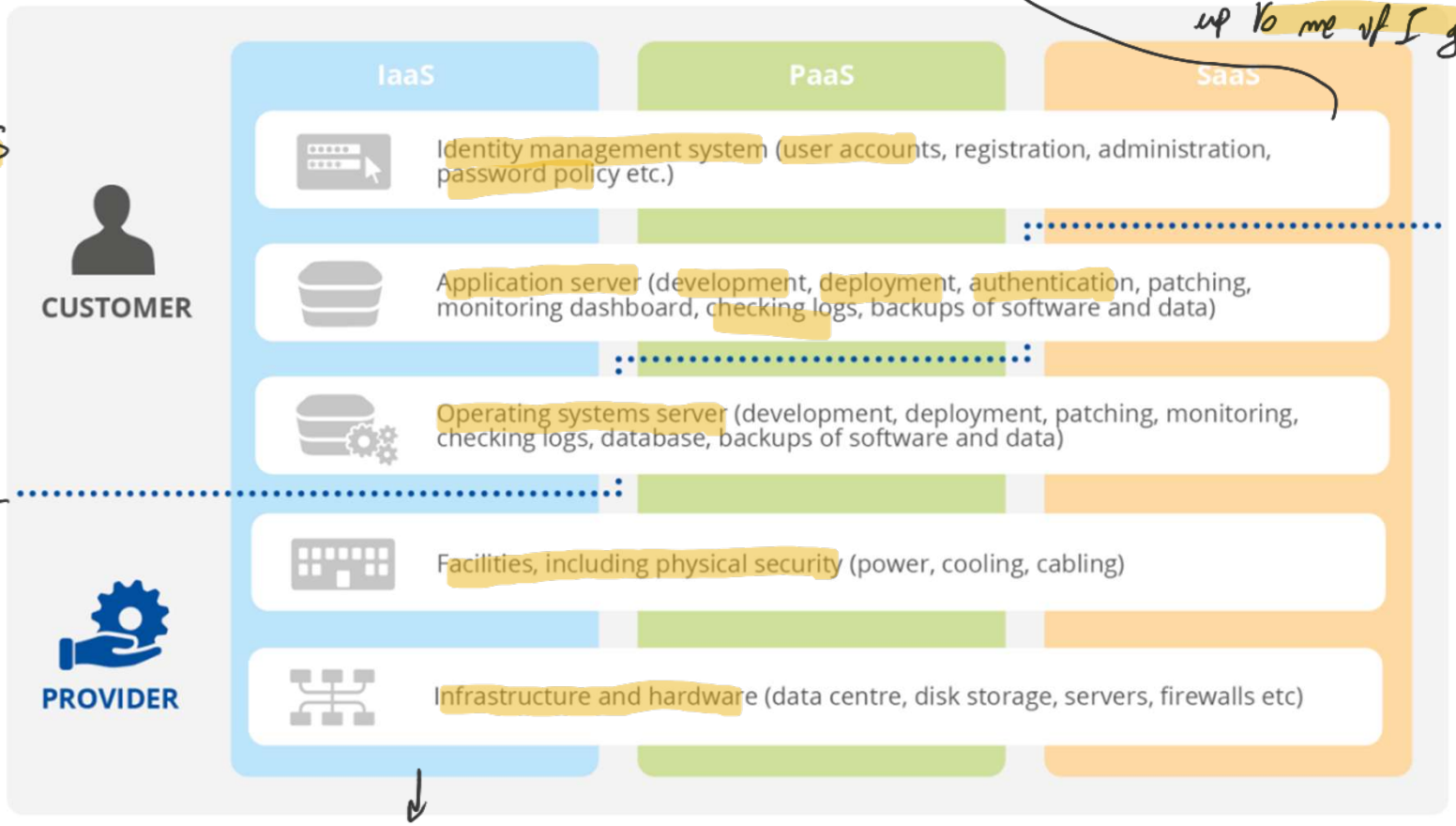
② Protecting cloud from outside

① There should not be any kind of network impact coming from the cloud.

For example: virus on my phone is able to access cloud computing infrastructure. But then this cloud can infect other people: so something comes in, then goes out again.

For sure for customer: if I'm showing PW, up to me if I get hacked.

Who is in charge for CS protection?



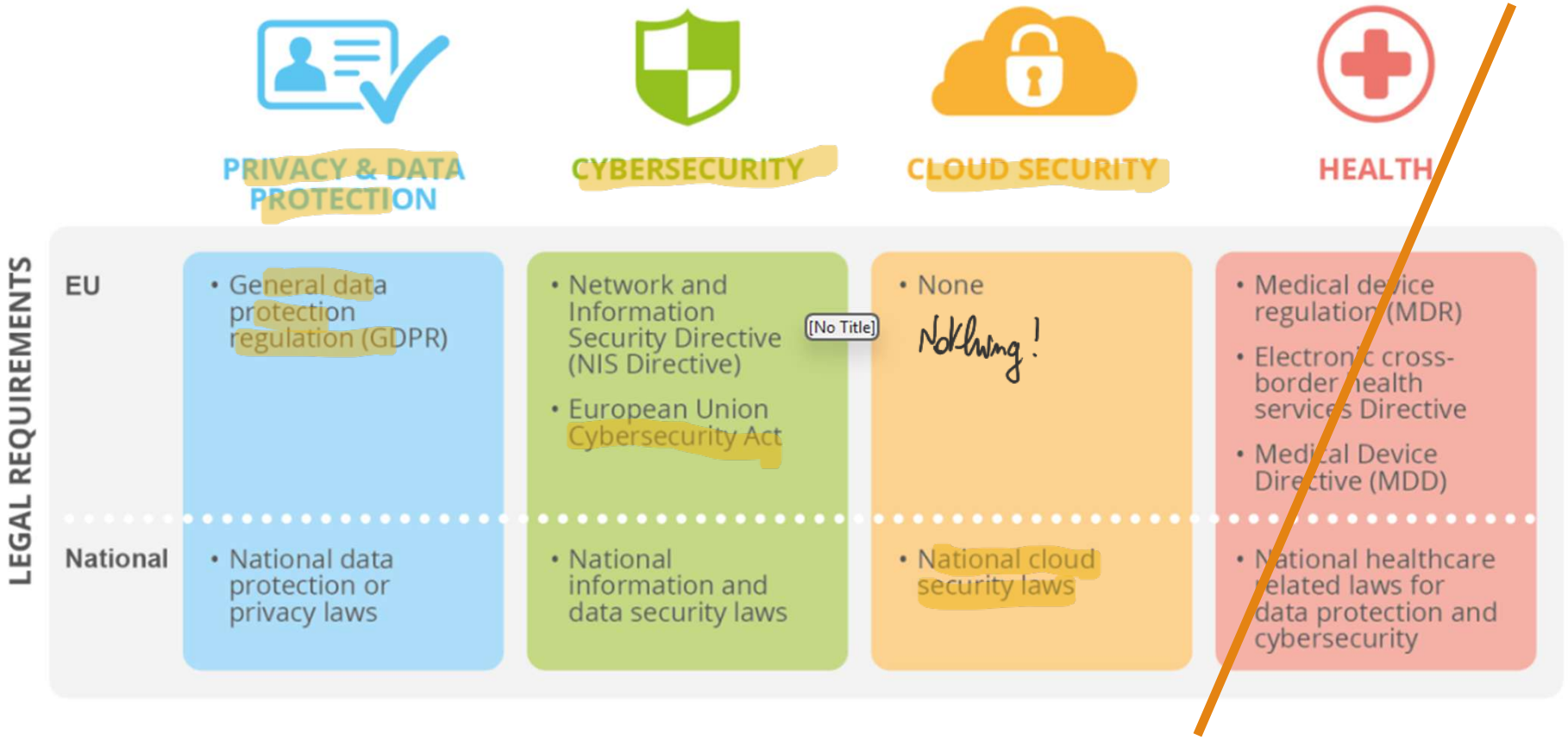
Usually always in charge of cloud

Provider giving the possibility to customer to use OS server, so it is up to them to check.

Who does what in terms of requirement. If we know this, we know who's in charge to comply with reg.

If I'm the provider, I have to look at this.

Provider of cloud computing, NIS applies. If I process, GDPR.



SPECIFIC FEATURES

availability but also integrity safeguarded

The Cloud contract includes a set of technical elements that applies regardless of the type of service covered by the contract itself:

1. the data are no longer stored on the user's 'physical' servers but are allocated on the provider's systems (except for local copies)
2. the service provider's infrastructure is shared among many users (multi-tenant model), so adequate levels of security are essential
3. use of the service is via the web through the Internet, which therefore assumes a central role for the quality of the services used and supplied
4. services that can be acquired from the service provider are on a pay-as-you-go basis to cope with any needs that may arise with elastic and simplified implementation systems (e.g. when more disk space or more computing power is needed).

↑ safeguarding confidentiality

CC should have reliable internet connection so availability is guaranteed.

make cloud available 24/7.

(4) If I'm paying for a service, doesn't matter if I use it for 1 hour or 24 hour, price is same. Or, I can pay for a specific amount of resources.

How does sys work?

The Cloud contract includes a set of technical elements that applies regardless of the type of service covered by the contract itself:

1. the data are no longer stored on the user's 'physical' servers but are allocated on the provider's systems (except for local copies)

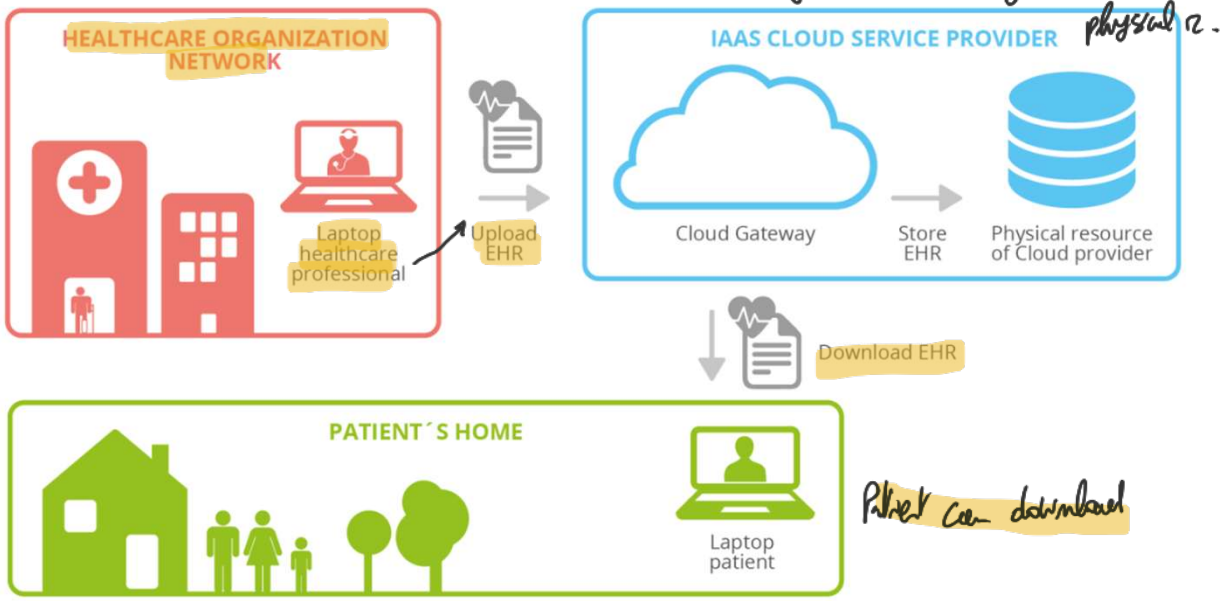
2. the service provider's infrastructure is shared among many users (multi-tenant model), so adequate levels of security are essential

3. use of the service is via the web through the Internet, which therefore assumes a central role for the quality of the services used and supplied

4. services that can be acquired from the service provider are on a pay-as-you-go basis to cope with any needs that may arise with elastic and simplified implementation systems (e.g. when more disk space or more computing power is needed).

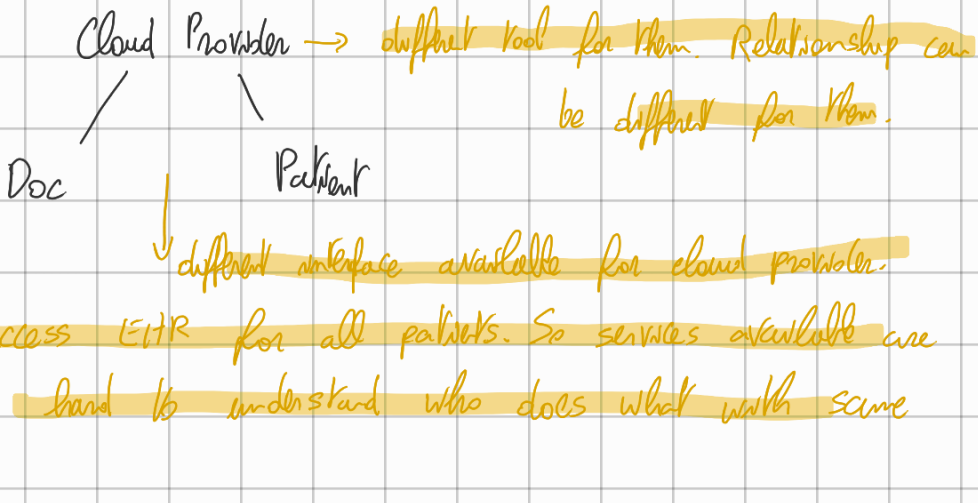
Figure 1: Cloud Architecture Model - Electronic Health Record (EHR)

goes via cloud gw, stored via physical rz.



Patient can download

You might have additional actor:



EX: doctor can access EHR for all patients. So services available are different. Can be hard to understand who does what with same cloud system.

@ They are uploaded from doc to the CC server.

DEFINITION OF PROCESSING OPERATION AND ITS CONTEXT

Personal data processed	Contact information (patient's last and first name, address, telephone number, email address), contact information of relatives for emergency cases, social insurance number, medical appointments, medical examination results, pathologies, allergies, diagnosis and treatment plans (medical information), administrative and financial information (invoices, hospitalisation papers, etc.).
Processing Purpose	Provision of healthcare services (diagnosis, treatment, hospitalisation), treatment planning and billing
Data Subject	Patients, relatives, doctors, nurses
Recipients of the Data	Doctors and nurses, administration and accounting department, public health system, patients
Data Processor	IaaS Cloud service provider

@ all these included in Health care record

↳ Still personal data

↳ financial information

doctor recognisable

↳ I can access my record

↳ need to let my employer know

ones that receive data through healthcare record

Good step forward for GDPR.

Data processing

data controller is the hospital because is in charge of the provision.

So, CC service is the processor, not the controller. If there's a data breach, data processors need to inform controllers. And it's the controller that is in charge to report!

But processor is the one that should provide info.
Controller should adopt tech/org. measures, but controller doesn't have physical responsibility!
So here there will be a shared responsibility in this sense. What if processor has not adopted measures? The contractual agreement between controller and processor is the safeguard for controller because they can't know what's going on.*

Data protection challenges

Privacy by design techniques : ex. make sure that data processor adopt and applies measures explained by GDPR.

Data management

Data deletion

Data portability

* Contractual agreement ensures the highest level of control and security for data!

② We have different actors possibly! And managing data can become tricky; transfer of data from one party to another. Data flow is extremely delicate.

③ How difficult is to erase accounts on social: what happens if I withdraw consent (GDPR); data can be connected: mother and me with genetic diseases.

④ Hospital changes the Cloud Computing provider. You have to have the possibility to move your data from one place to another. This is crucial for interoperability for EHR too for example, that's easy for that sector.

Cybersecurity challenges

- Access control.
- Audit.
- Authorisation.
- Availability.
- Chain of trust / chain of responsibility.
- Compliance.
- Confidentiality.
- Cybersecurity incident management.
- Identification and authentication.
- Integrity.
- Multi-tenancy.
- Network security.
- Privacy.
- Storage.
- Transparency/visibility/nonrepudiation.

NIS 2: CC services as Essential Entities. So they need Tech. and org. measures to protect the security of overall system. Article 32 will be contractually allocated to processor, but this is on them. Comply with sets of stand.: supply chain security etc.

Cybersecurity architecture in cloud computing

↳ if you have an incident this is on them.

EX: data breach report is on controller, but in parallel possibly report to CSIRT.

Access Control	Controls access to data and systems through authentication and authorization mechanisms.	Authentification and authorization
Encryption	Converts data into a coded format to prevent unauthorized access, applied to data at rest and in transit.	Applied to different levels (storage, network or application)
Data Backup & Recovery	Ensures data can be recovered in the event of a breach or system failure, stored in a secure location.	Data backups in separate cloud service or on-premise data center
Network Security	Protects against cyber attacks and unauthorized access.	firewalls, IDS/IPS, and VPNs
Compliance	Adherence to relevant regulations and standards, like GDPR and PCI DSS, is vital for strong cybersecurity NIS	Can also be a requirement for the CC service. Can be shared.

So a lot of obligation.

Most common/important measures to be adopted. 1. User needs to know when PW. But up to CC provider to ensure auth and authoriz. measures! * Possible to connect this to anonymisation for personal data

Pseudonymisation: changed the data to not make them connected to data subject but with possibility to reconnect.

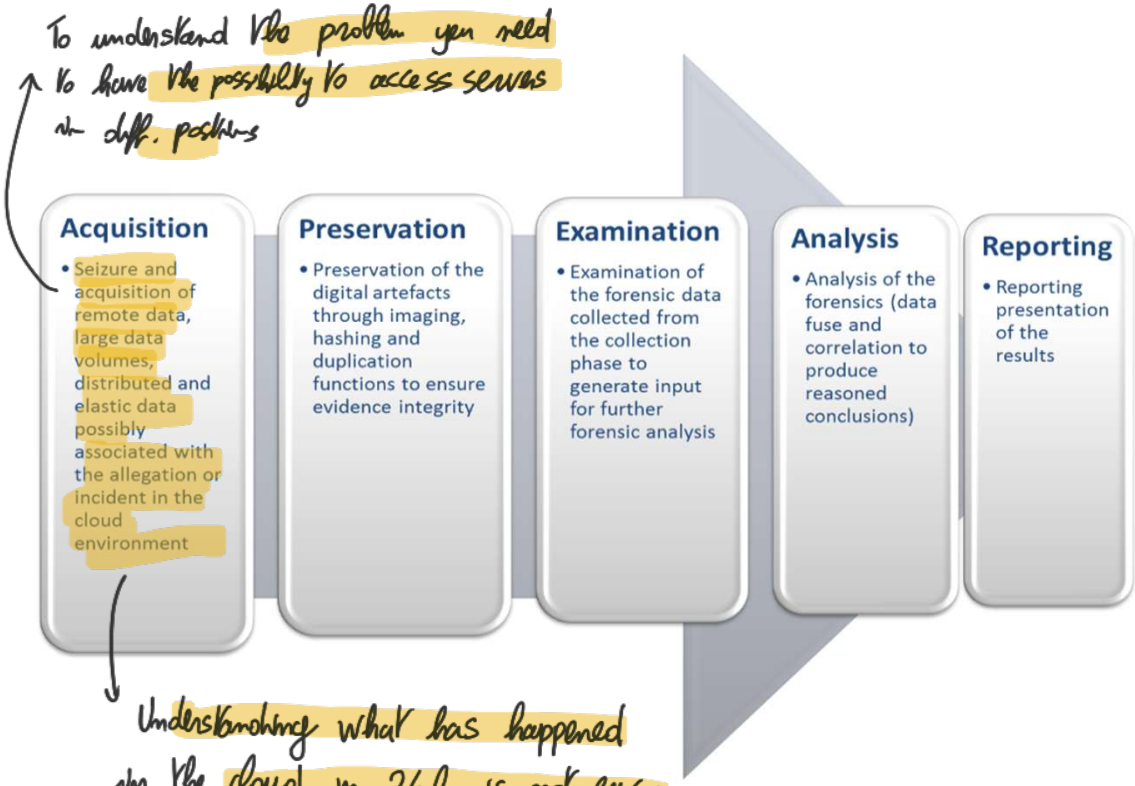
Anonymisation disconnects info from the Data Subject. In that case, encryption is not even needed for data protection but might be needed for sys security.

③ Ensuring availability and recover in case of failure!

Cybersecurity challenges

Cloud forensic stages

Whenever a case for attack, you can have forensic stages to understand what is going on in the cloud: in CC system, find out who has done what is hard.



Understanding what has happened in the cloud in 24h is not easy.
You should understand what has been attacked.
Who might have been shared, so integrity of evidence might get compromised.
Incident evaluation is even more difficult.