

# Secure Electronic Health Record Mechanism Supporting Privacy- Preserving Cloud Outsourcing

Chun-I Fan

Distinguished Professor

Department of Computer Science and Engineering

National Sun Yat-sen University, Taiwan



# Innovation and Significance

## Privacy-Preserving Medical Data Warehouse System Supporting Secure Data Mining

### FHIR (Fast Healthcare Interoperability Resources)

- **Trend of Medical Data Cloudization**
- Global trends in healthcare development: Smart healthcare, precision medicine, and remote care
- Cross-Platform Medical data: webpages, Apps, healthcare information systems, wearable devices

### Protection of **Medical Data Privacy with Encryption**

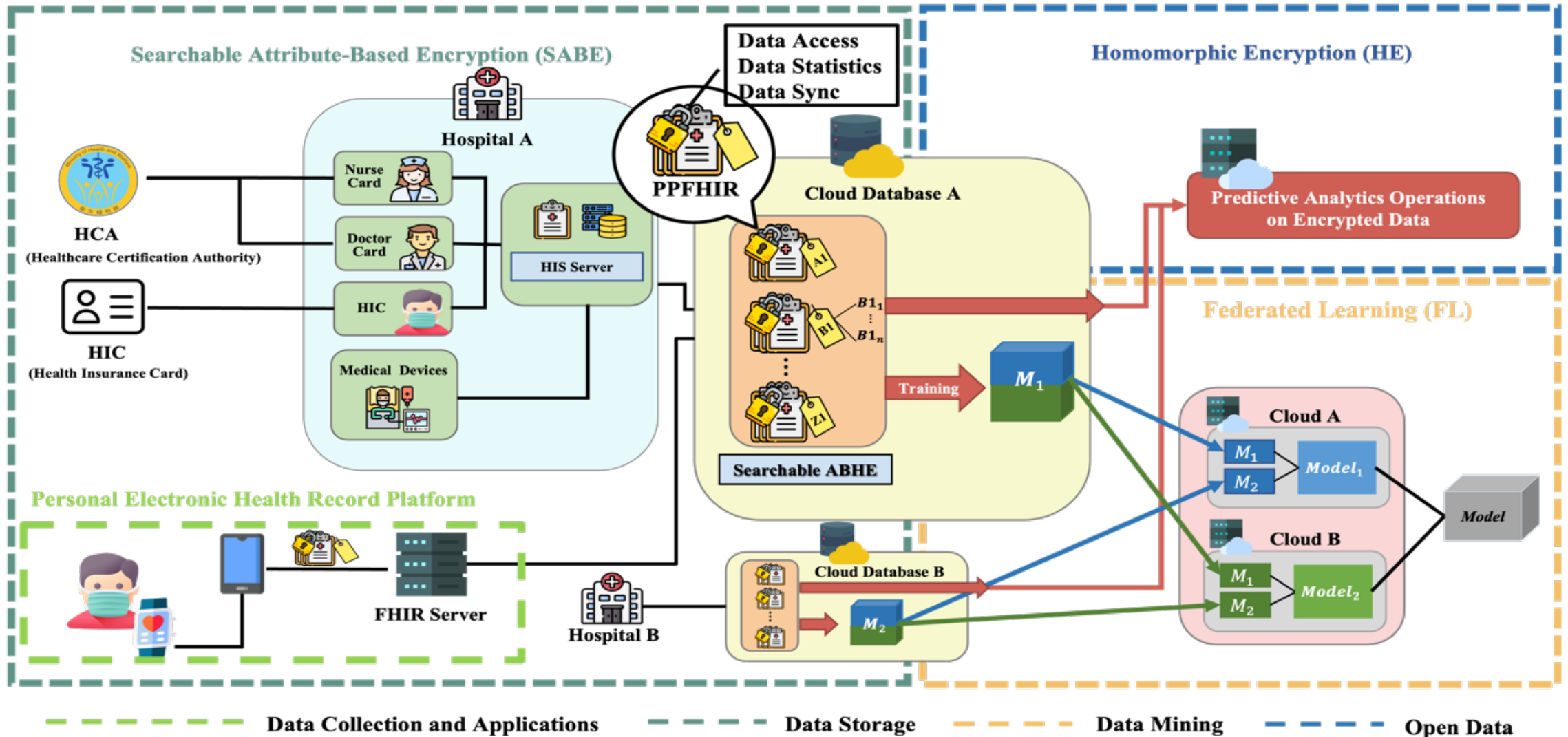
- **Compliance with Regulations**
- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act

### Preventing **Insider Attacks** and **Public Cloud Snooping**

- Research and technology primarily focused **on mitigating external threats.**

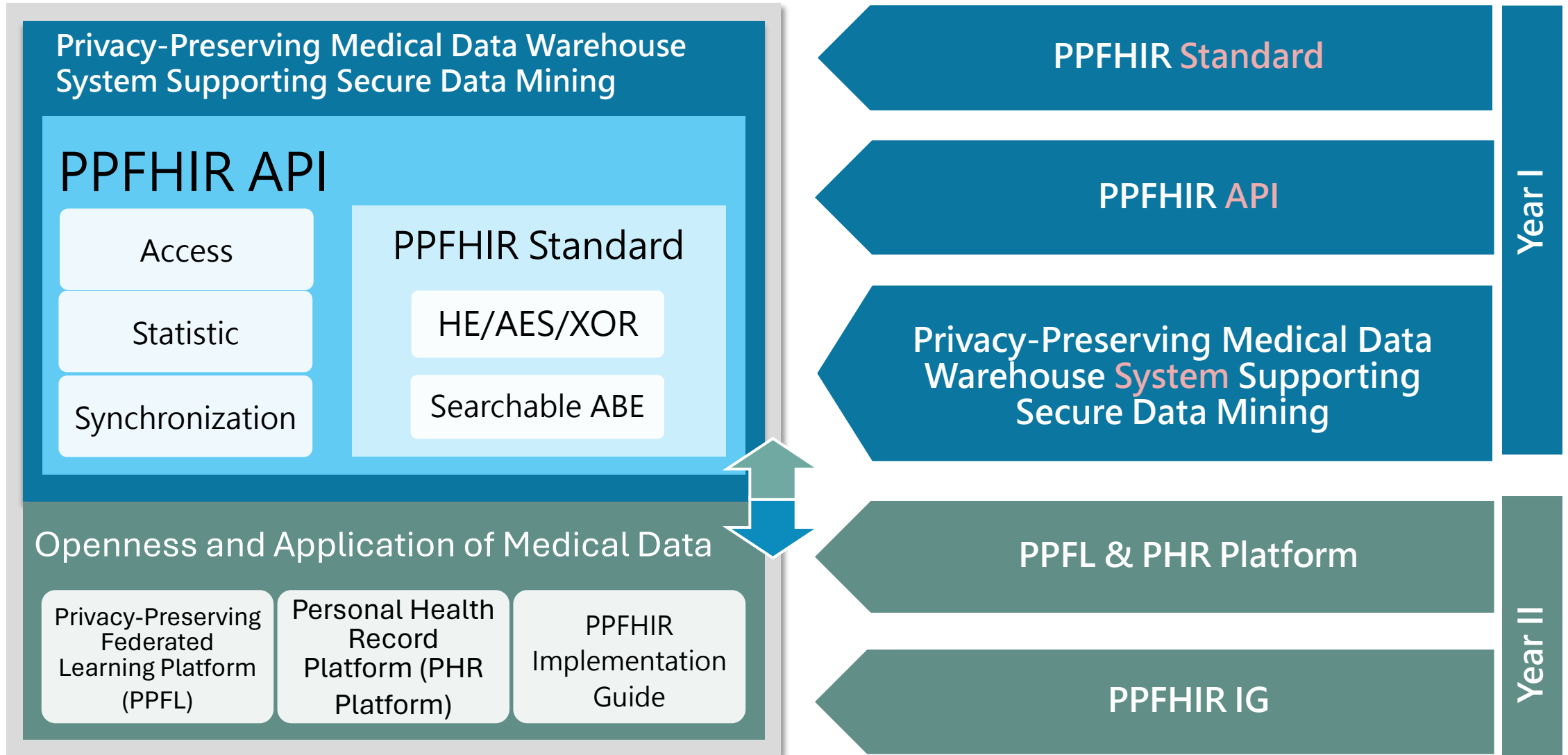
# System Architecture

## Privacy-Preserving Medical Data Warehouse System Supporting Secure Data Mining



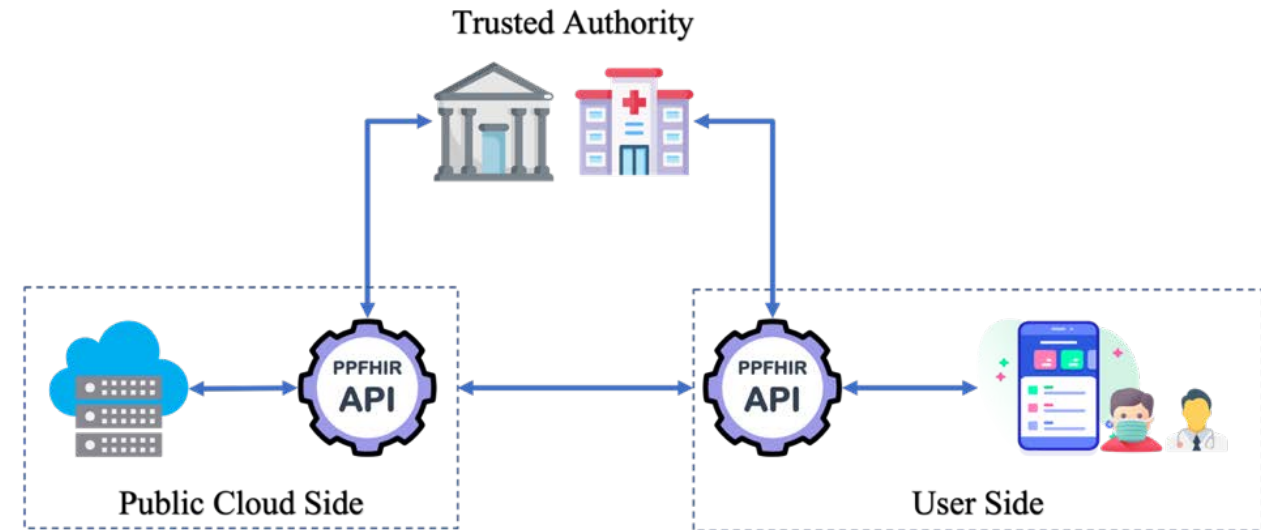
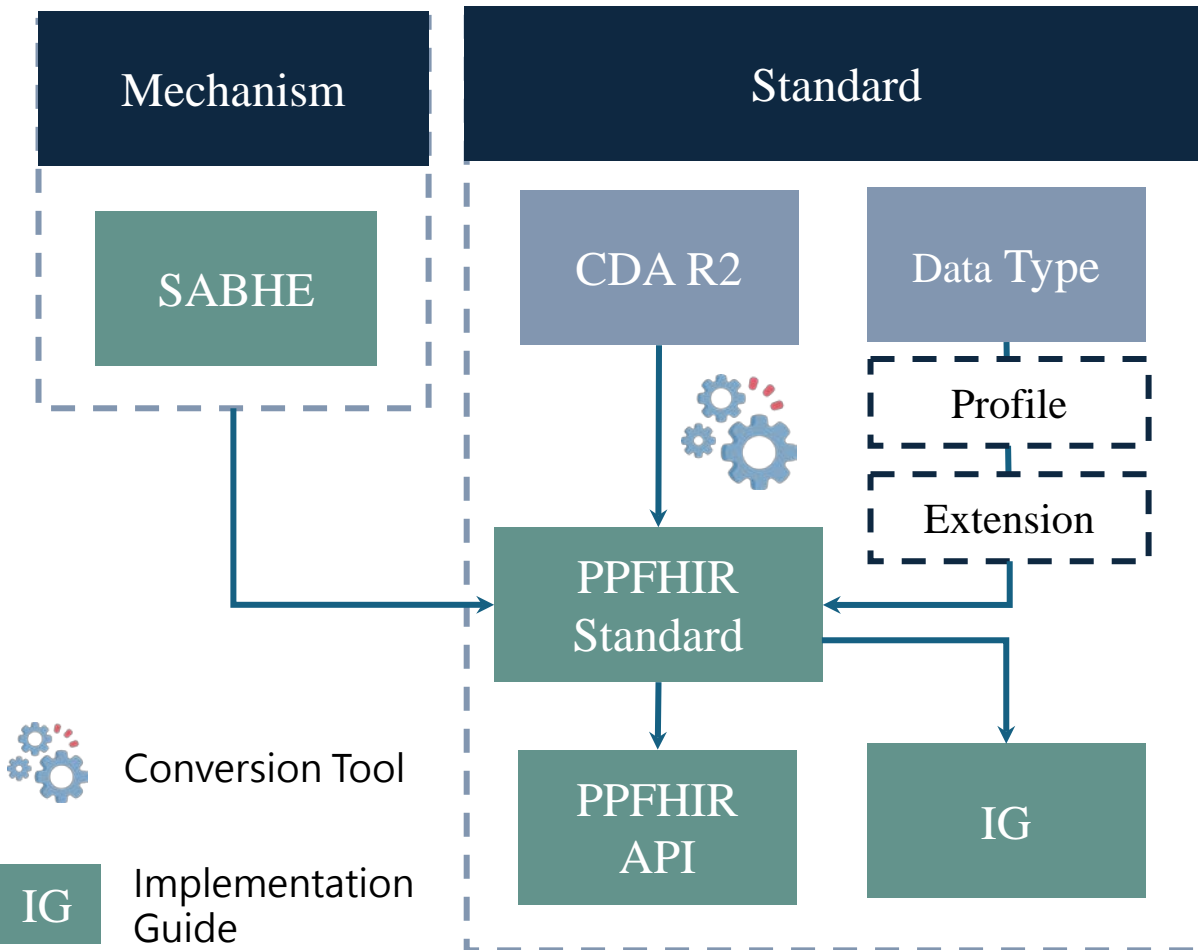
# Output and Results

- **SABHE**: Searchable Attribute-Based Homomorphic Encryption
- **ABHPRE**: Attribute-Based Homomorphic Proxy Re-Encryption
- **PPFHIR**: Privacy Preserving Fast Healthcare Interoperability Resources



# Introduction to Research and Development Technologies

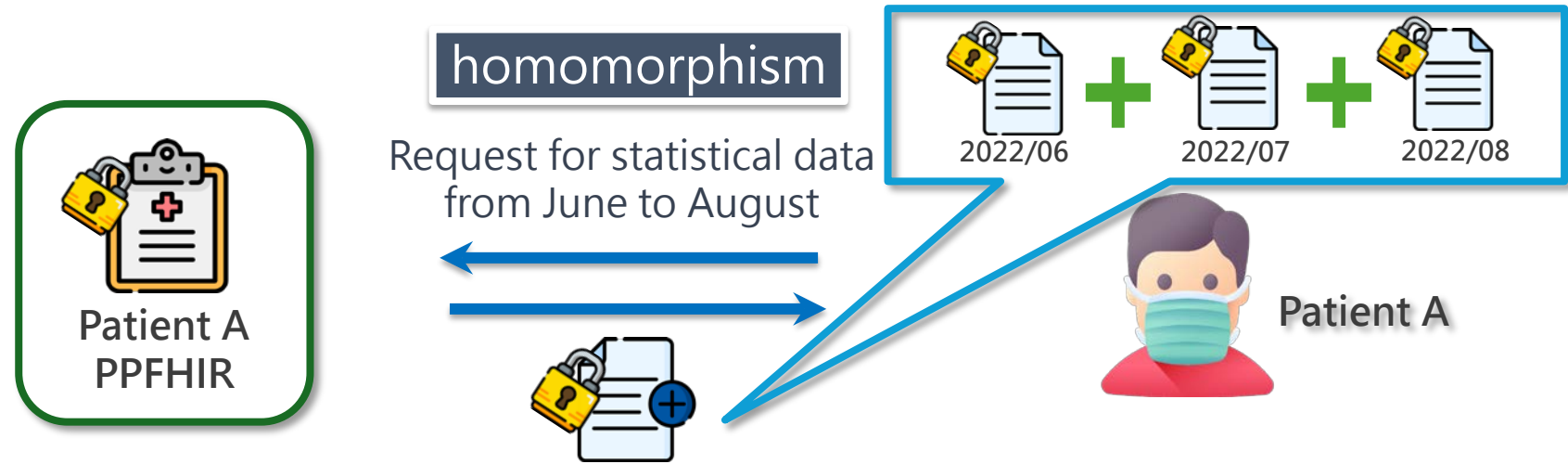
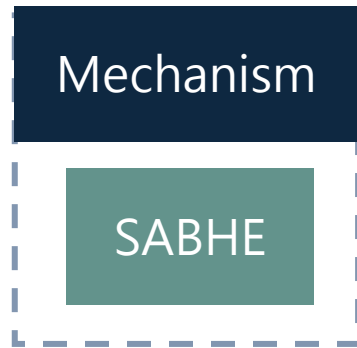
## Privacy-Preserving FHIR (PPFHIR)



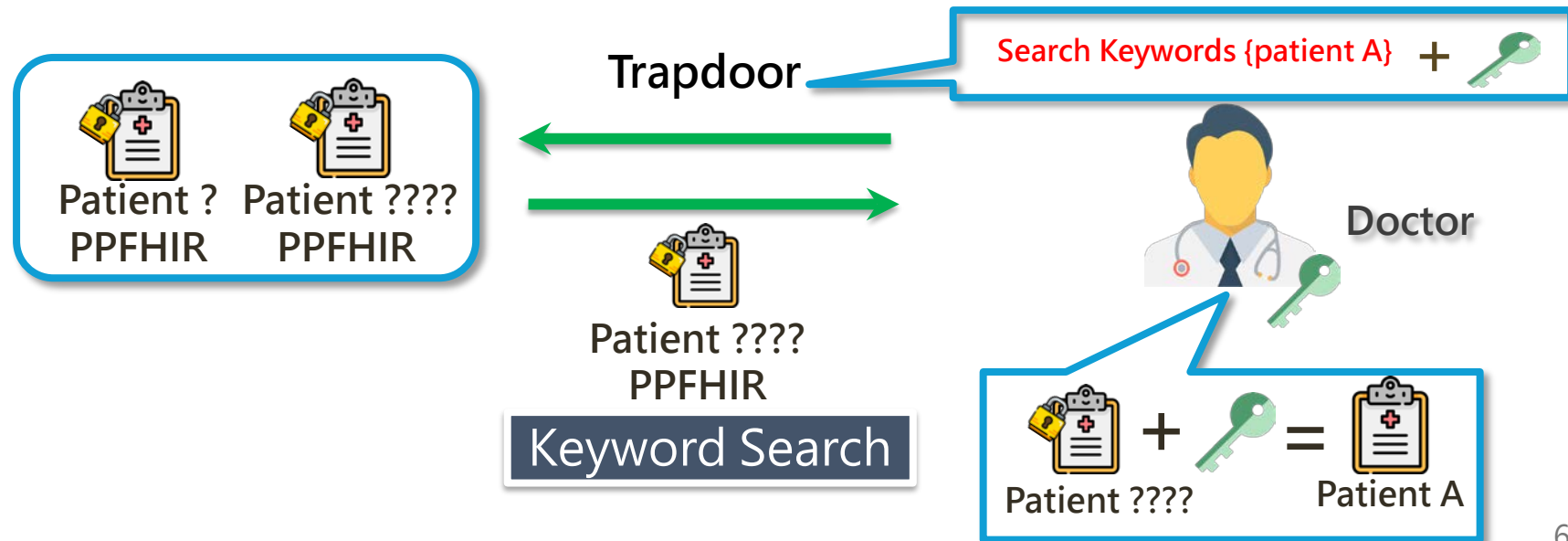
The PPFHIR API is available for any healthcare institutions and stakeholders who have adopted the FHIR standard. It seamlessly **integrates its current systems with the PPFHIR system**, facilitating secure cloud-based medical data storage.

# Introduction to Research and Development Technologies

## Privacy-Preserving FHIR (PPFHIR)



Searchable **Attribute-Based Homomorphic Encryption (SABHE)** allows for secure data storage in ciphertext form on a public cloud while providing three key features: **Attribute-Based Encryption, Homomorphic Computation, and Searchability**



# Introduction to Research and Development Technologies

## Privacy-Preserving FHIR (PPFHIR)

### Statistics

Blood Pressure

Range: 2022-12-01 ~ 2022-12-31

Amount: 150

Systolic Average: 124 mm[Hg]

Diastolic Average: 81 mm[Hg]

Observation Type

Blood Pressure

Statistics Range

2022-12-01

2022-12-31

December 2022

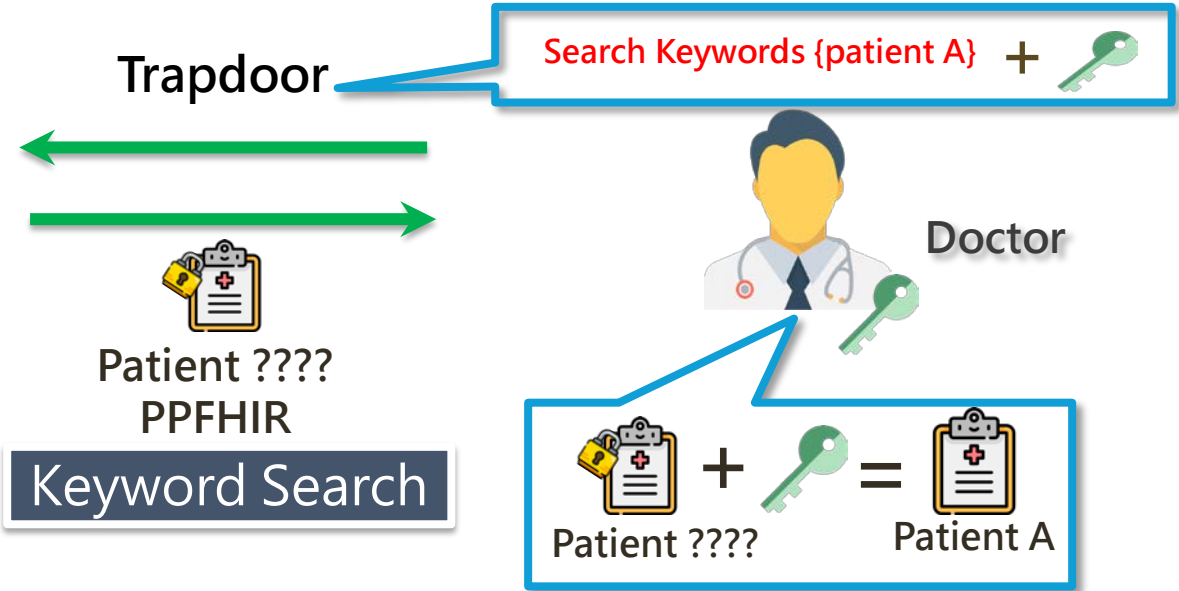
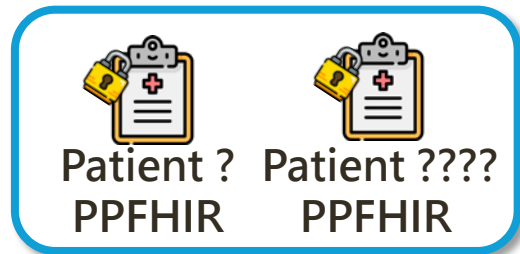
Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24

```

資訊 PPFHIRServer.PPFHIRServer doHomomorphic - Search for Homomorphic Ciphertext by name: mOHW
資訊 PPFHIRServer.PPFHIRServer doHomomorphic - Found ciphertext at id: 10094
資訊 PPFHIRServer.PPFHIRServer doHomomorphic   ciphertext: 110988143319085024066449066508511936927437519903968991803566965...
資訊 PPFHIRServer.PPFHIRServer doHomomorphic - Found ciphertext at id: 10094
資訊 PPFHIRServer.PPFHIRServer doHomomorphic   ciphertext: 158153553168152069517190100815088211172848359575437506670366617...
資訊 PPFHIRServer.PPFHIRServer doHomomorphic - Found ciphertext at id: 10095
資訊 PPFHIRServer.PPFHIRServer doHomomorphic   ciphertext: 776328054022215390048636823618936550606519627795819950687975759...
資訊 PPFHIRServer.PPFHIRServer doHomomorphic - Found ciphertext at id: 10095
資訊 PPFHIRServer.PPFHIRServer doHomomorphic   ciphertext: 276204798547694449041536863550198817864529937627218839867396061...
資訊 PPFHIRServer.PPFHIRServer doHomomorphic - Found ciphertext at id: 10096
資訊 PPFHIRServer.PPFHIRServer doHomomorphic   ciphertext: 836858086957357927350733472247794603742520155427096676663539743...
    
```

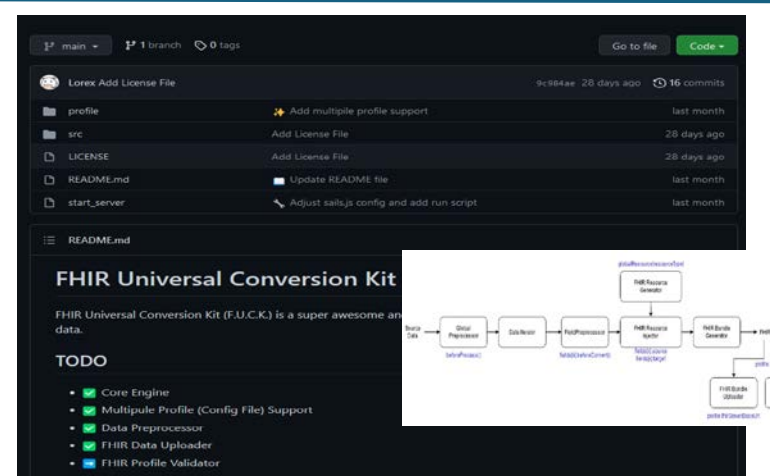
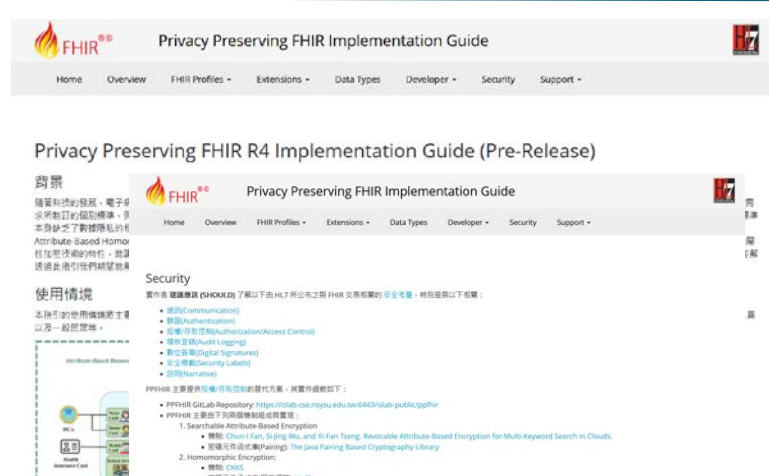
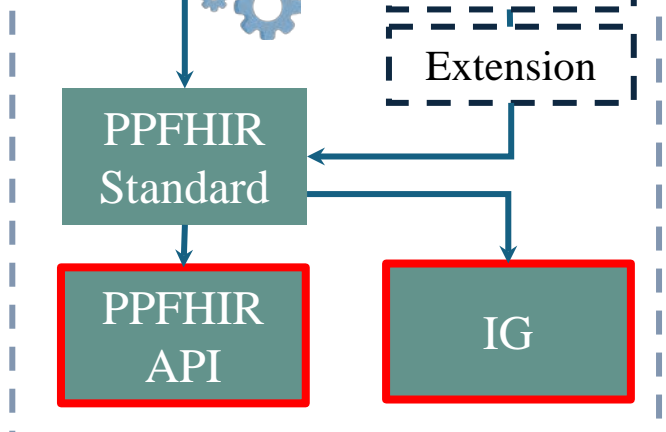
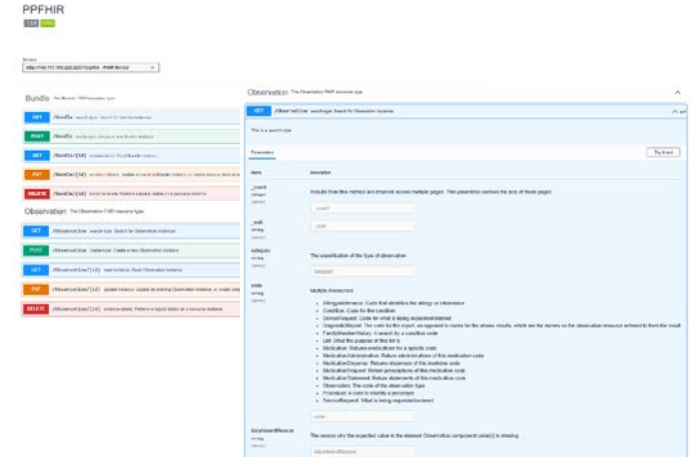
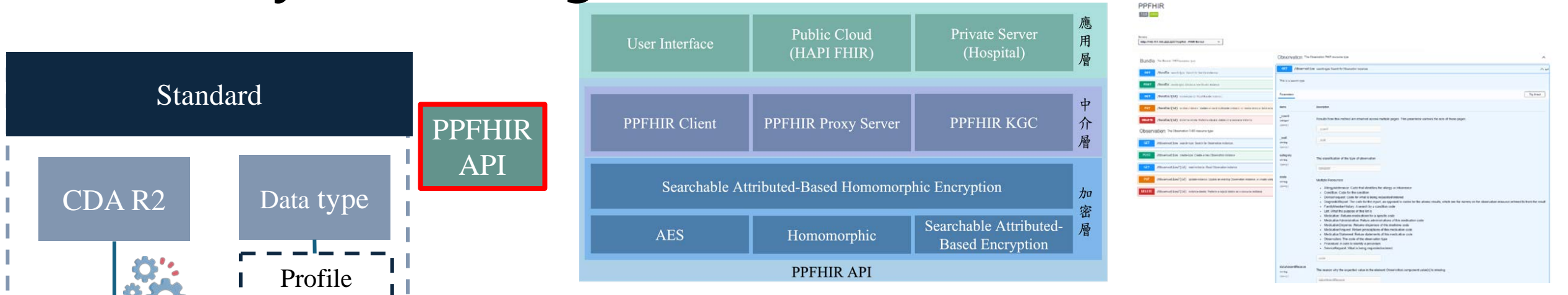
```


資訊 PPFHIRServer.PPFHIRServer doHomomorphic - Calculate the result.
資訊 PPFHIRServer.PPFHIRServer doHomomorphic - Result = 3335896267785818541270569462415721386297076278388172012798221704026099720336874447
4861858590082163412460735604091216739172540269985317834201244552317205461273465061835484213469495842947230999395218611709520664788991965324627594
9936573408400078537002653604137769423815156659812611253792855873754204852246193406331649801772000285546633090770483178807990841963384779637174016
資訊 PPFHIRServer.PPFHIRServer doHomomorphic - Second Result = 180028945918567597654700022189795219039383601838611893517518686847360900274
4262907685832052788794004305369942312100641783572760302985833930977409697703534058053889210692687829129928935584365466883585448643649878610991247
7340146558243834908350177567873542097732820046922896859125053741468287960601824330525197944144072006879698822169283837320370950828749421868943155
5
    
```




# Introduction to Research and Development Technologies

## Privacy-Preserving FHIR (PPFHIR)



 Conversion Tool

 Implementation Guide

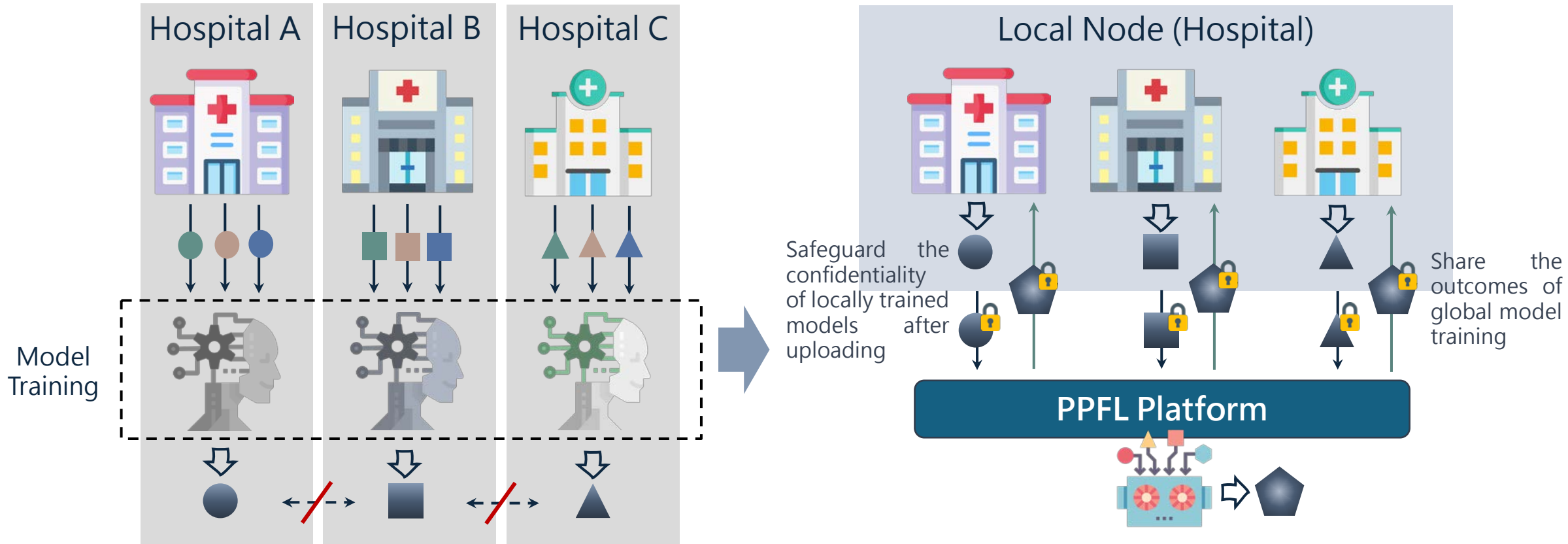
**【Implementation Guide】**  
Introduction to PPFHIR, Data Types, Profiles, Extensions, and Security Standards

**【PPFHIR Conversion Tool】**  
CDA R2 to PPFHIR Format Conversion System and Process Diagram



# Introduction to Research and Development Technologies

## Privacy-Preserving Federated Learning (PPFL)



Hospitals were **limited to training their models** within their respective institutions, which posed challenges to collaboration among multiple medical institutions.

Federated learning addressed this problem, which enables **collaboration among multiple medical institutions** and provides additional features such as **contribution verification**.

# Introduction to Research and Development Technologies Personal Health Record Platform

Partner Company "Doctor" Health Watch

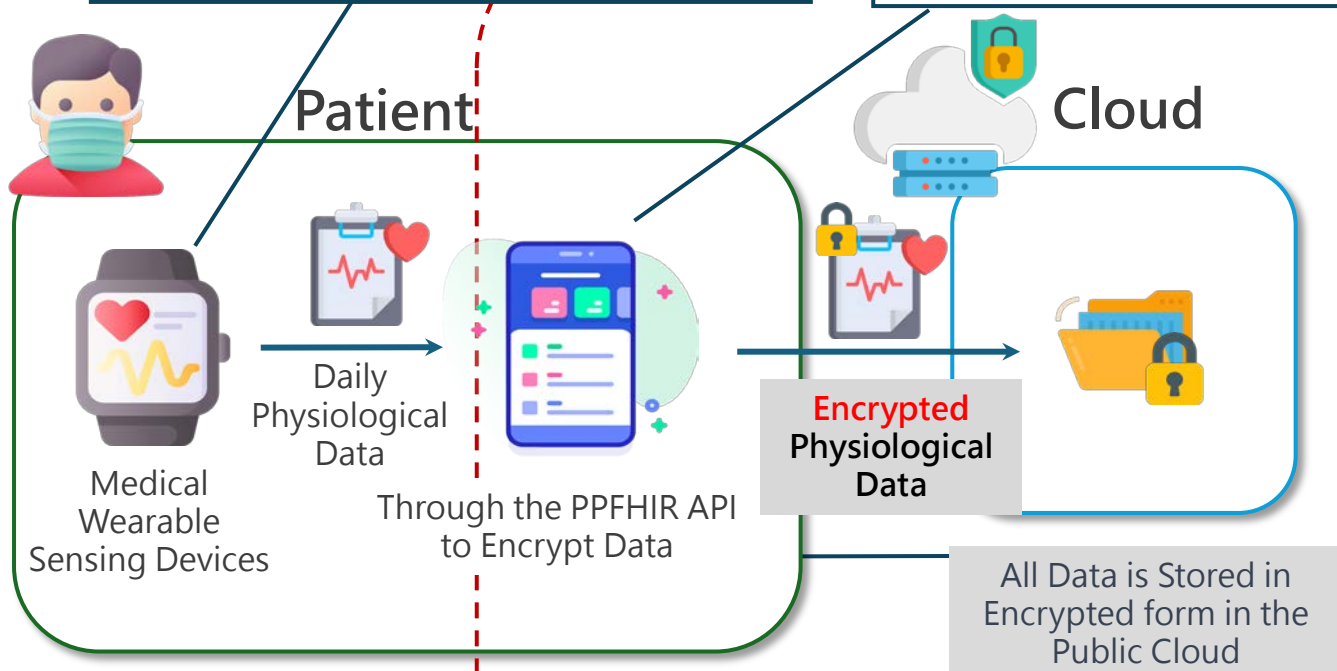
血壓 血氧濃度 體溫 睡眠 運動

Sensing Data → FHIR → PPFHIR

```

    {
      "id": "https://hl7.org/fhir/observation/997",
      "resource": "Observation",
      "meta": {
        "version": "1",
        "lastUpdated": "2022-09-17T08:16:59.308460100",
        "source": "http://hl7.org/fhir/observation/997",
        "system": "http://hl7.org",
        "code": "99795a-170b-47c2-827a-f02a4d85542"
      },
      "status": "completed",
      "category": "Vital Signs",
      "coding": [
        {
          "code": "99795a-170b-47c2-827a-f02a4d85542",
          "display": "Oxygen saturation in Arterial blood by Pulse oximetry"
        }
      ],
      "subject": "Patient/997"
    }
  
```

Flowchart: Source Data → Global Preprocessor (beforeProcess) → Data Inhibitor → FieldPreprocessor (beforeConvert) → FHIR Resource Injector (beforeInject) → FHIR Bundle Generator → FHIR Data → FHIR Bundle Uploader (beforeUpload) → API Response (beforeSaveData)



## PPFHIR API

### PPFHIR

1.0.5 OAS3

Bundle The Bundle FHIR resource type

- GET** /Bundle search-type: Search for Bundle instances
- POST** /Bundle create-type: Create a new Bundle instance
- GET** /Bundle/{id} read-instance: Read Bundle instance
- PUT** /Bundle/{id} update-instance: Update an existing Bundle instance, or create using a client-assigned ID
- DELETE** /Bundle/{id} instance-delete: Perform a logical delete on a resource instance

Add Search Modify Delete

Privacy-Preserving Medical Data Warehouse System Supporting Secure Data Mining

# Introduction to Research and Development Technologies

## Personal Health Record Platform

### Basic Information

**Patient ID**  
9998

**Name**  
吳曉鳳

**Gender**  
male

**ID Card**  
E741852963

**Phone**  
0945678912

**Email**  
qweasdzxc@gmail.com

**Birth Date**  
1979-04-12

**Address**  
高雄市鹽埕區大勇路130號

[Edit](#)







```
Result Body Raw Message
{
  "resourceType": "Patient",
  "id": "9998",
  "meta": {
    "versionId": "1",
    "lastUpdated": "2023-01-14T13:41:31.850+00:00",
    "source": "#7uFjjdhVhSue57d4"
  },
  "text": {
    "status": "generated",
    "div": "<div xmlns='http://www.w3.org/1999/xhtml'><div class='hapiHeaderText'>wV3R7Q2YDwqNIIiEht<b>IYHC+z/77WMW0YLFJRJDYFCPBXYMYUCEE5F1V4LWA8HG= </b></div><table class='hapiPropertyTable'><tbody><tr><td>wgKUDbdzsEwXAMequf5qv18NNC9XFhpqaUB+OgLv2xY= </td></tr><tr><td>Address</td><td><span>6nu+WvwZi8Yk5dCHD6XX0m8+kOVIrNMYIRqmRMUwg= </span></td></tr><tr><td>Date of birth</td><td><span>HjFhYGQcDFxrg127zRRnq/j7fHmF4G8gLO1gFH0sMXo= </span></td></tr></tbody></table></div>"
  },
  "identifier": [ {
    "use": "usual",
    "value": "wgKUDbdzsEwXAMequf5qv18NNC9XFhpqaUB+OgLv2xY="
  } ],
  "active": true,
  "name": [ {
    "use": "usual",
    "text": "z/1Y00rFDGDe9w2+gSwWQUJdGCSqITkiIzdwZVhMfgg=",
    "family": "iYhc+z/77wmW0YLFJRJDYFCPBXYMYUCEE5F1V4LWA8HG=",
    "given": [ "wV3R7Q2YDwqNIIiEhbSARUkgltqEyt6NbbQX1Meo0w=" ]
  } ],
  "telecom": [ {
    "system": "phone",
    "value": "4zNBGJ4V0L3Rc8WCy/LTW8awX1dIu05mwTaKW/wCeLo=",
    "use": "mobile"
  }, {
    "system": "email",
    "value": "w6J0wzRftpcRteY99bWkhq1Lq1sokYEyY38MLZi2yy8ZrVPG7o6HhuQcDK60Y9Sp",
    "use": "home"
  } ],
  "gender": "male",
  "birthDate": "8368-04-20",
  "address": [ {
    "use": "home",
    "type": "postal",
    "line": [ "6nu+WvwZi8Yk5dCHD6XX0m8+kOVIrNMYIRqmRMUwg=" ],
    "city": "HjFhYGQcDFxrg127zRRnq/j7fHmF4G8gLO1gFH0sMXo=",
    "district": "wDw2wdsEM1YdEzAgTWSbmyud4n+Kpg053zjnw0m7d1k="
  } ],
  "contact": [ {
    "name": {
      "use": "usual",
      "text": "ObwQXLADUQEMJcNEHxno00aMh044Fhu1B0zF1bUIzWI=",
      "family": "/MAKEKTLI56b3RiaUYp7+Lnhv239M2C7d6rPCA9mxb0=",
      "given": [ "+w+3ST2lydiABA12RtFBLecYDRzQeulQMXZHLK94H8I=" ]
    }
  }, {
    "telecom": [ {
      "system": "phone",
      "value": "aR5HNN8v3710GKjjrhXD05f0+wp2pNoMagp0xGIChdY=",
      "use": "mobile"
    } ]
  } ]
}
```

User Interface

Encrypted Medical Records in the Public Cloud

# Highlights and Breakthroughs



-  **World's First** Secure Cloud Access for FHIR Medical Data Enabled by Functional Encryption Technology
-  **First in Taiwan** to publish a standard document on FHIR implementation guidelines with privacy protection mechanisms (IG)
-  **Secure medical data exchange system** based on PPFHIR
-  PPFHIR integrates **encryption, ciphertext search, homomorphic computing, and access control** through the SABHE (Searchable Attribute-Based Homomorphic Encryption) mechanism.
-  PPFHIR **compatible with existing FHIR systems**
-  **Privacy-Preserving Federal learning** is achieved.

新聞

## 電子病歷上雲法規正式上路了! 4大重點法規速覽

電子病歷上雲目的：醫療AI、資安、遠距醫療

Official Announcement of Taiwan's Regulations for  
Cloud-Based Electronic Medical Records  
(Medical AI, Information Security, Telemedicine)

# Highlights and Breakthroughs



**NSTC** 國家科學及技術委員會  
National Science and Technology Council

獎 狀

國立中山大學范俊逸特聘教授及研究團隊參與國家科學及技術委員會前瞻及應用科技處「臺灣資安卓越深耕-學術型資安研究計畫」111年度期末成果發表會，發表「具隱私保護暨安全資料探勘之醫療資料倉儲系統」計畫成果，表現卓越，並深受其他研究團隊肯定，茲頒發「最亮成果獎」，以資鼓勵。



前瞻資安科技專案計畫辦公室主持人 鄧惟中  
中華民國 112 年 3 月 24 日



2023 FutureTech Award



20th National Innovation Award

The Brightest  
Achievement  
Award

# Industry-Government-Academia Cooperation

## Ministry of Health and Welfare

## Kaohsiung Veterans General Hospital

First year  
Technology promotion, and  
cooperation



會議過程

- 「具隱私保護安全資料驅動之醫療資料會談表」
- 「具隱私保護安全資料驅動之醫療資料會談表」
- 「具隱私保護安全資料驅動之醫療資料會談表」
- 會談
- 會議重點
  - 衛福部承辦針對 PPFHIR 提出多項 Implementation 具體表採用，未來編修有機會可以協助研「具」驅動之醫療資料會談表，所提出的「具」(提供)。
  - 「具隱私保護安全資料驅動之醫療資料會談表」應公開標準與其使用的加密技術與方法。
  - 「具隱私保護安全資料驅動之醫療資料會談表」功能增加密性可能有關算法的代理，因此件能提升外，可搭配特殊硬體或商業合作件 (Package)，來提供技術與標準。

資料驅動之醫療資料會談表此的計畫關係可以... 具隱私保護安全資料驅動之醫療資料會談表此的計畫關係可以...

Second Year  
Cooperation



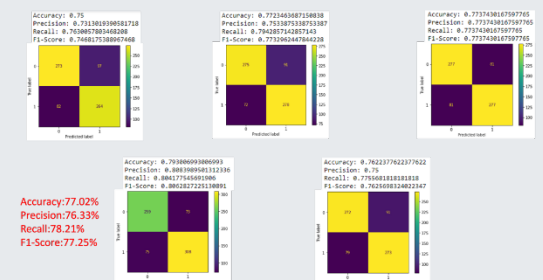
Study on the possibility of introducing PPFHIR technology into the "Risk Alert Platform" of the Ministry of Health and Welfare for information security recommendations.

First year  
Technology promotion, and  
cooperation



Strategic alliance agreement between National Sun Yat-sen University and Kaohsiung Veterans General Hospital.

Second Year  
Cooperation



PPFL Analysis of Pre- and Intra-operative Data.

A scenic landscape at sunset. The sun is low on the horizon, casting a warm glow over the scene. In the foreground, there is a lush green forest with a winding path. In the middle ground, a large body of water reflects the sunset. In the background, there are rolling mountains under a cloudy sky. The text "Thank You!" is overlaid in the center of the image.

Thank You!