RECOMMENDED REFORMS IN THE PRACTICE OF OBTAINING INFORMED CONSENT FOR SHARING MEDICAL AND HEALTH DATA

Shinto TERAMOTO, Prof.
Faculty of Law, Kyushu University, Fukuoka, Japan
teramoto.shinto.717@m.kyushu-u.ac.jp
shin.teramoto@terrara.net

2024 SUSTAINABLE INDUSTRIAL PROCESSING SUMMIT AND EXHIBITION

The Rise of Medical and Healthcare Collaboration - Domestic and Cross-Border

- Telemedicine: Medical professionals collaborating across borders to provide care.

- SaaS Health Apps: Smartphone apps for health management used across multiple countries, often with language and legal adaptations.

- SaMD: Software as a Medical Device, often a type of SaaS, increasingly approved by regulatory authorities.

- Data Sharing is Essential: These trends highlight the need for cross-border sharing of medical and health information.

TEMDEC Telemedicine Development Center of Asia
International Medical Department, Kyushu University Hospital

Transmitting the Latest Medical Care Information
From Fukuoka to Asia and the World

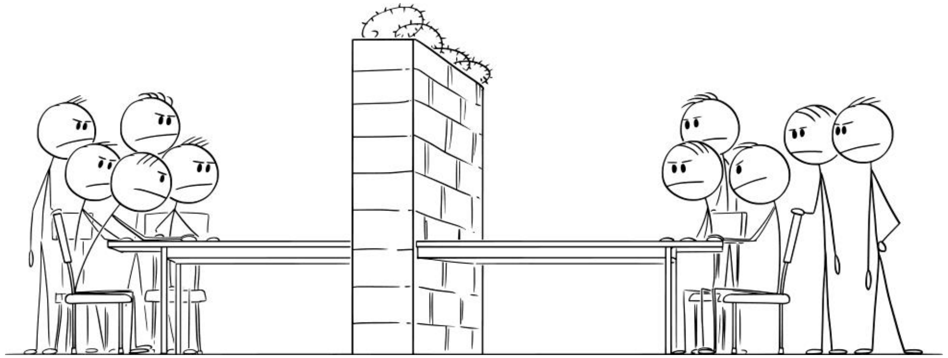
Challenges for Medical and Healthcare Data Sharing - Personal Information Protection Law

- Data Sharing is Essential for Healthcare: Effective healthcare depends on the ability to share medical and health information both domestically and internationally.

- Personal Information Protection Laws Hinder Data Sharing: Current laws prioritize data privacy, creating barriers to necessary or beneficial data sharing.

- Burden on Healthcare and Medical Providers: Healthcare and Medical providers face challenges navigating complex and often conflicting legal frameworks, whether domestically or across different jurisdictions.

- Potential Harm to Patients and Individuals: Legal barriers to data sharing can negatively impact patient care, limit access to treatments, and hinder everyday health management for individuals.



Challenges for Medical and Healthcare Data Sharing - Personal Information Protection Law

- Current Laws Are Overly Stringent: Current personal information protection laws impose an unreasonably high burden of proof on medical and healthcare providers, thereby hindering data sharing even when beneficial for patient care or public health.

- Shifting the Burden of Proof: Shifting the burden of proof to the data subject to demonstrate unnecessary data sharing could facilitate greater data sharing. However, this necessitates legal reforms in multiple jurisdictions which create implementation barriers.

Clue to Possible Solutions

- Focus on Existing Legal Framework:
  - Existing personal information protection laws generally permit data sharing among entities that have individually obtained prior informed consent from the data subject.
- Streamline Informed Consent:
  - Implement a system that enables data subjects (including patients) to provide informed consent directly to each entity seeking to share their personal information, utilizing secure information and communication technology.
- This would facilitate data sharing while respecting individual autonomy.

Clue to Possible Solutions

- Domestic Laws Alone Are Not Enough: Medical and healthcare services increasingly operate across borders, thus amending only domestic laws cannot fully address data sharing challenges.
- International Harmonization: While international treaties or agreements are a long-term goal, more immediate solutions are needed.
- De Facto Standards: Establish and promote de facto standards for informed consent and data sharing that can be adopted across different jurisdictions.

Scenario for Designing a Solution

- Actors:
  - P: a data subject (individual)
  - I_P: a specific piece of personal information belonging to P
  - E_1: an entity (institution, company, etc.)
  - E_2: another entity
- Suppose:
  - E_1 obtains I_P from P with P's informed consent; and
  - E_1 intends to share I_P with E_2.

Scenario for Designing a Solution

- Platforms:
  - PKI (Public Key Infrastructure) to authenticate:
    - The identities of P, E_1, and E_2; and
    - Their respective manifestations of intent (consent, refusal, withdrawal of consent, confirmation of consent, etc.).
  - SCH (Secure Communication Hub): A telecommunication infrastructure that can liaise and temporarily store and time-shift communications between the persons or entities whose identities are authenticated by the PKI.

Procedure Enabled by PKI and SCH

- Actors:
  - P: a data subject (individual)
  - I_P: a specific piece of personal information belonging to P
  - E_1: an entity (institution, company, etc.)
  - E_2: another entity
- Suppose:
  - E_1 obtains I_P from P with P’s informed consent; and
  - E_1 intends to share I_P with E_2.

Procedure Enabled by PKI and SCH

1. P gives E_1 informed consent to obtain I_P.

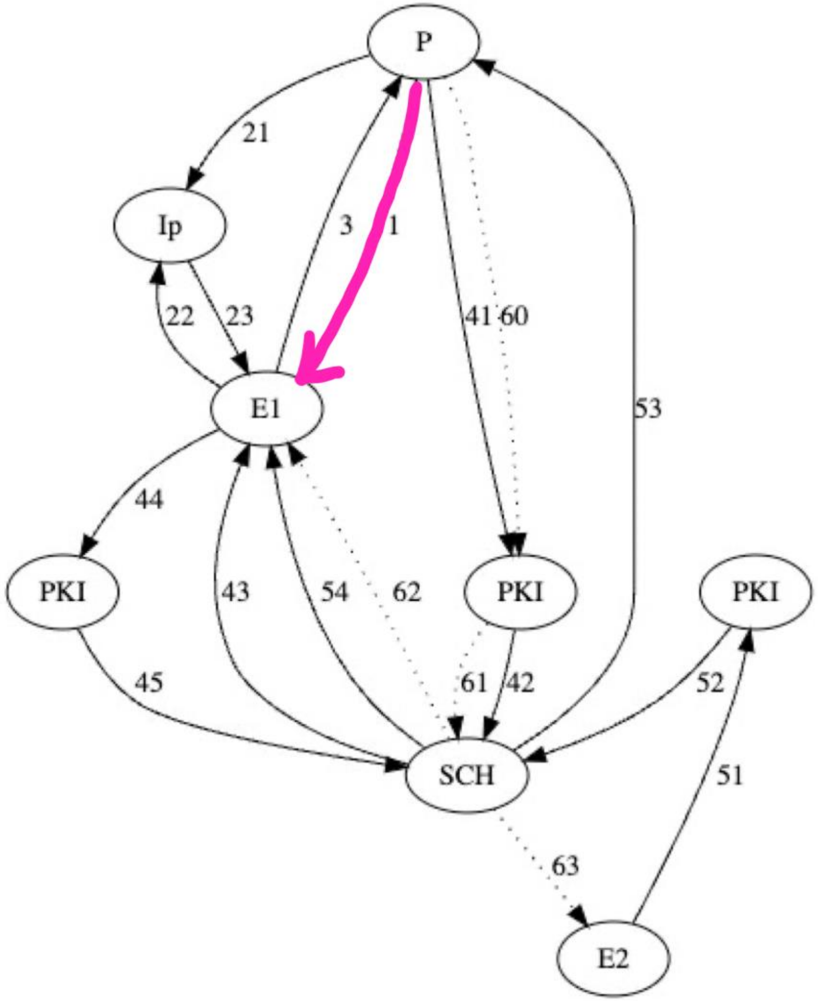
2. E_1 obtains I_P.

3. E_1 informs P of E_1's intention to share I_P with E_2 and provides E_2's identification.

4. P creates a message expressing P's consent, or revocable consent, for E_2 to obtain I_P from E_1. E_1 countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

5. Upon E_2 accessing P's message, SCH notifies both P and E_1.

6. SCH may be designed to allow P to withdraw or revoke P's consent.



Procedure Enabled by PKI and SCH

1. P gives E_1 informed consent to obtain I_P.

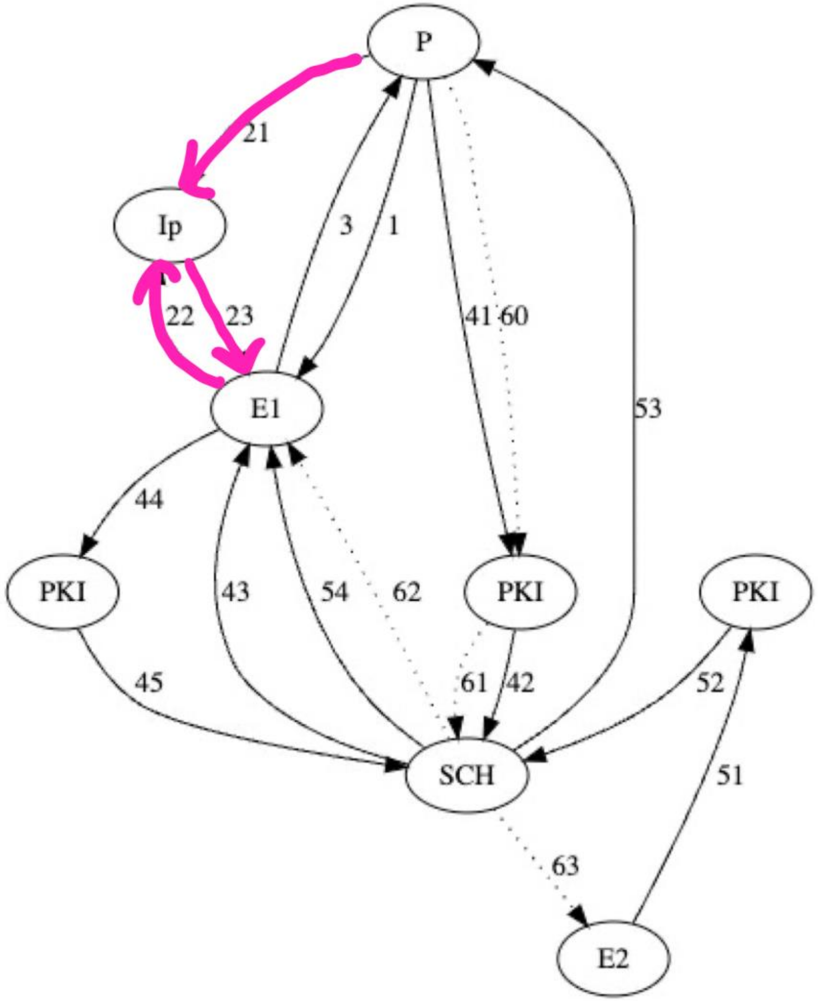
2. E_1 obtains I_P.

3. E_1 informs P of E_1's intention to share I_P with E_2 and provides E_2's identification.

4. P creates a message expressing P's consent, or revocable consent, for E_2 to obtain I_P from E_1. E_1 countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

5. Upon E_2 accessing P's message, SCH notifies both P and E_1.

6. SCH may be designed to allow P to withdraw or revoke P's consent.



Procedure Enabled by PKI and SCH

1. P gives E_1 informed consent to obtain I_P.

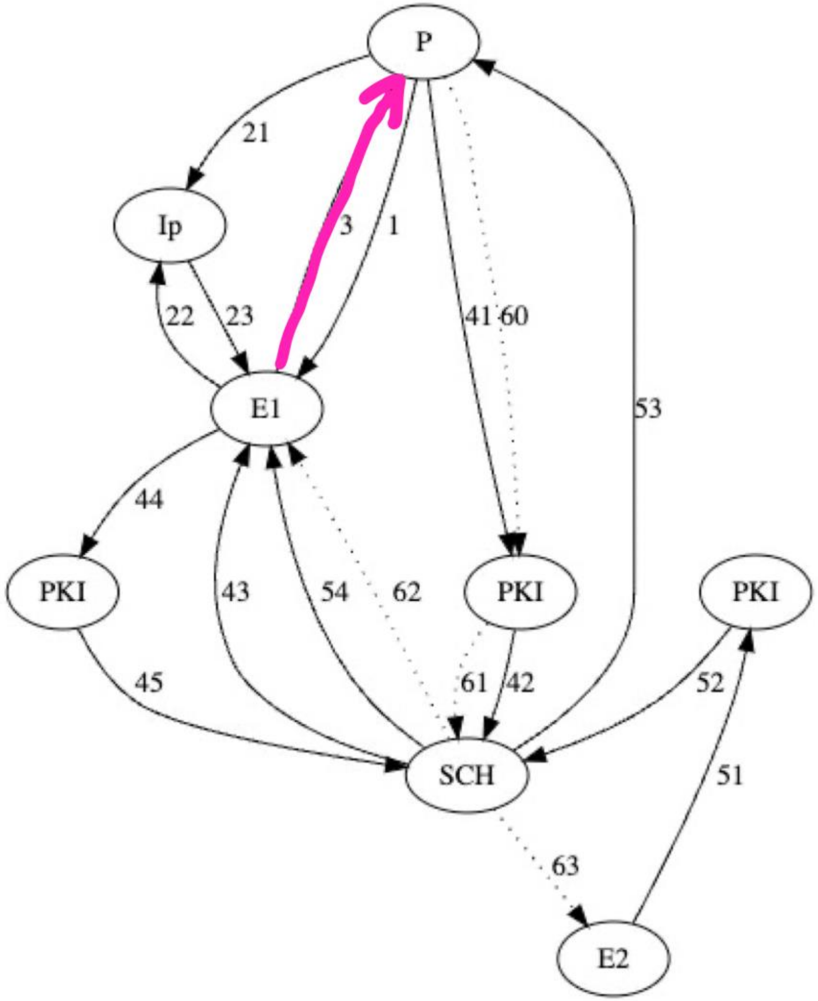
2. E_1 obtains I_P.

3. E_1 informs P of E_1's intention to share I_P with E_2 and provides E_2's identification.

4. P creates a message expressing P's consent, or revocable consent, for E_2 to obtain I_P from E_1. E_1 countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

5. Upon E_2 accessing P's message, SCH notifies both P and E_1.

6. SCH may be designed to allow P to withdraw or revoke P's consent.



Procedure Enabled by PKI and SCH

1. P gives E_1 informed consent to obtain I_P.

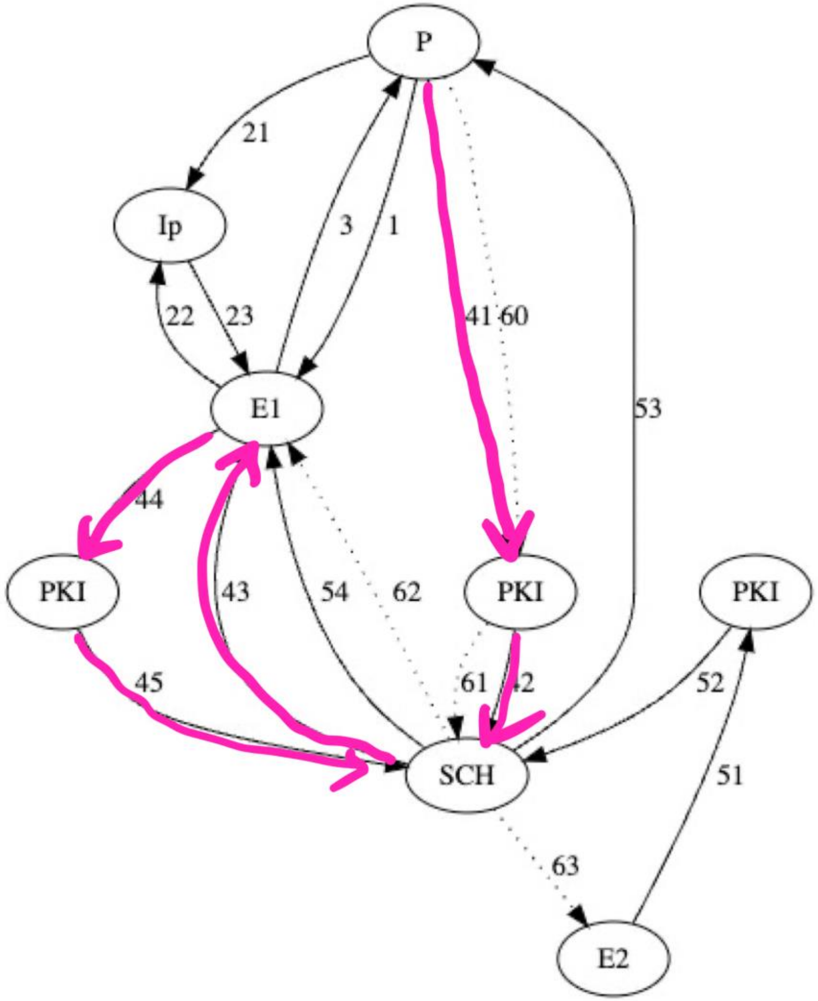
2. E_1 obtains I_P.

3. E_1 informs P of E_1's intention to share I_P with E_2 and provides E_2's identification.

4. P creates a message expressing P's consent, or revocable consent, for E_2 to obtain I_P from E_1. E_1 countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

5. Upon E_2 accessing P's message, SCH notifies both P and E_1.

6. SCH may be designed to allow P to withdraw or revoke P's consent.



Procedure Enabled by PKI and SCH

1. P gives E1 informed consent to obtain IP.

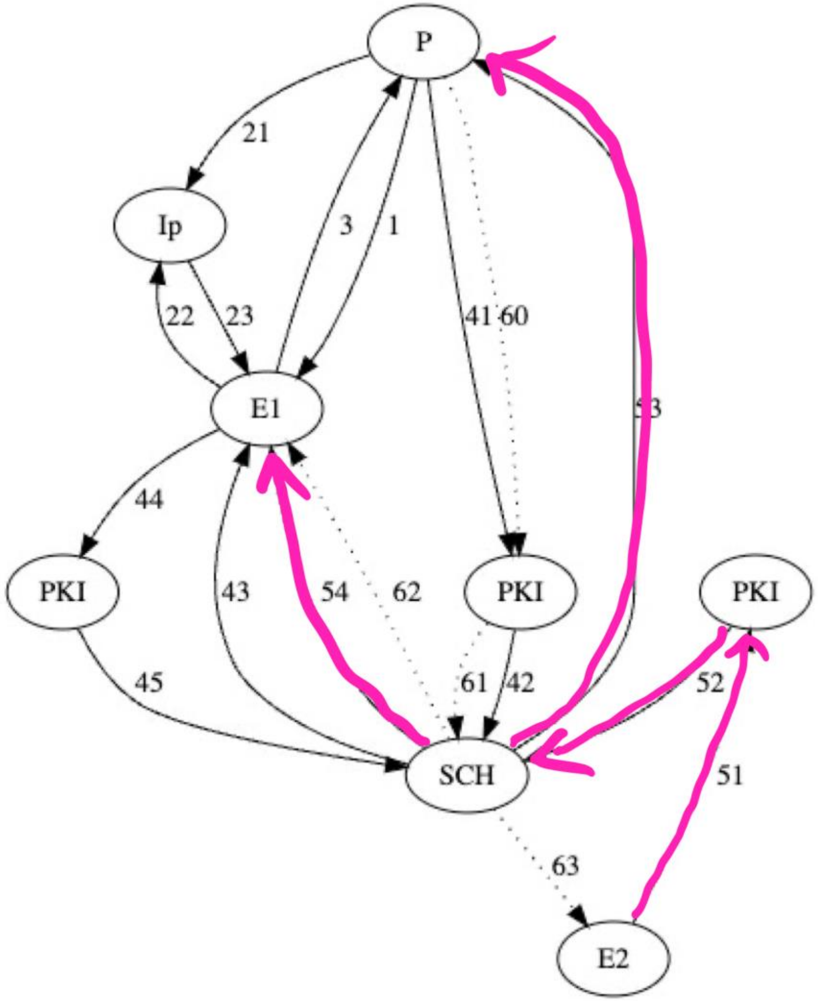
2. E1 obtains IP.

3. E1 informs P of E1's intention to share IP with E2 and provides E2's identification.

4. P creates a message expressing P's consent, or revocable consent, for E2 to obtain IP from E1. E1 countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

5. Upon E2 accessing P's message, SCH notifies both P and E1.

6. SCH may be designed to allow P to withdraw or revoke P's consent.



Procedure Enabled by PKI and SCH

1. P gives E_1 informed consent to obtain I_P.

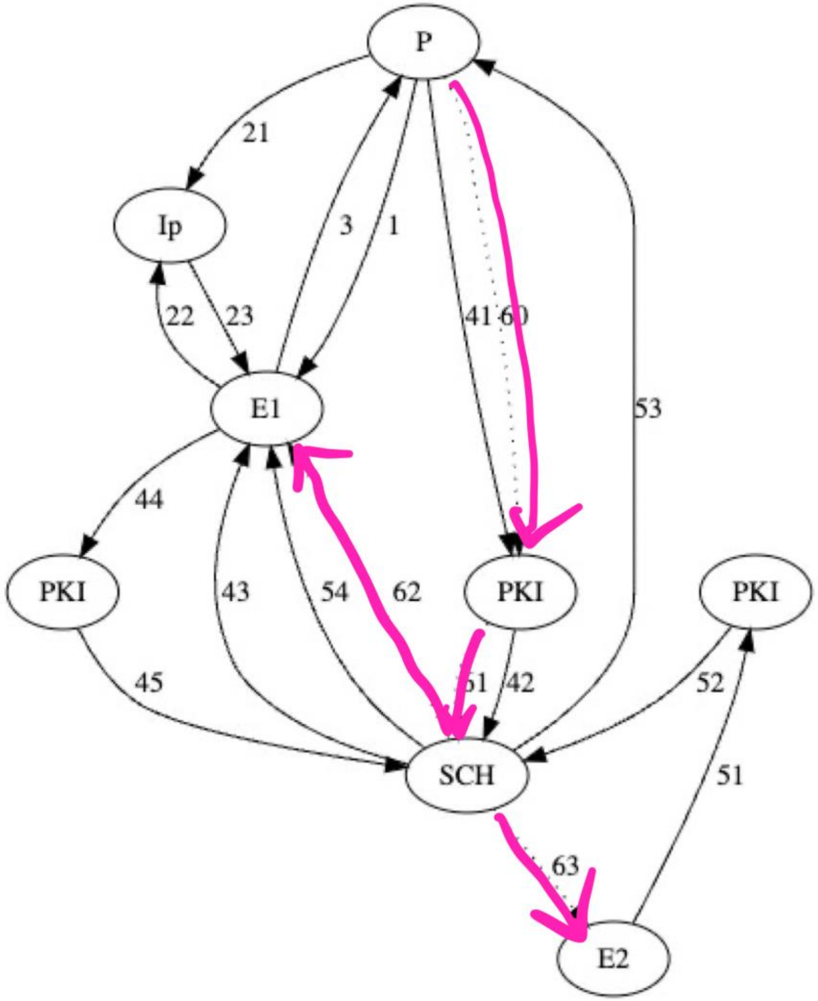
2. E_1 obtains I_P.

3. E_1 informs P of E_1's intention to share I_P with E_2 and provides E_2's identification.

4. P creates a message expressing P's consent, or revocable consent, for E_2 to obtain I_P from E_1. E_1 countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

5. Upon E_2 accessing P's message, SCH notifies both P and E_1.

6. SCH may be designed to allow P to withdraw or revoke P's consent.



Procedure Enabled by PKI and SCH

1. P gives E_1 informed consent to obtain I_P.

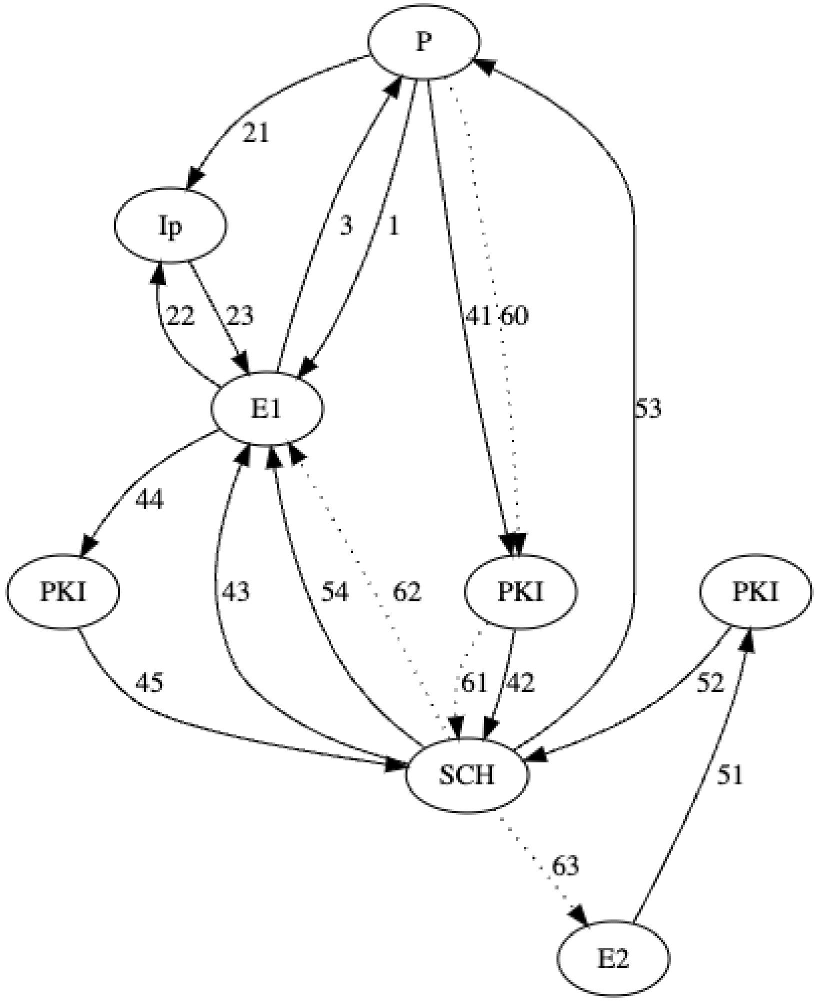
2. E_1 obtains I_P.

3. E_1 informs P of E_1’s intention to share I_P with E_2 and provides E_2’s identification.

4. P creates a message expressing P's consent, or revocable consent, for E_2 to obtain I_P from E_1. E_1 countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

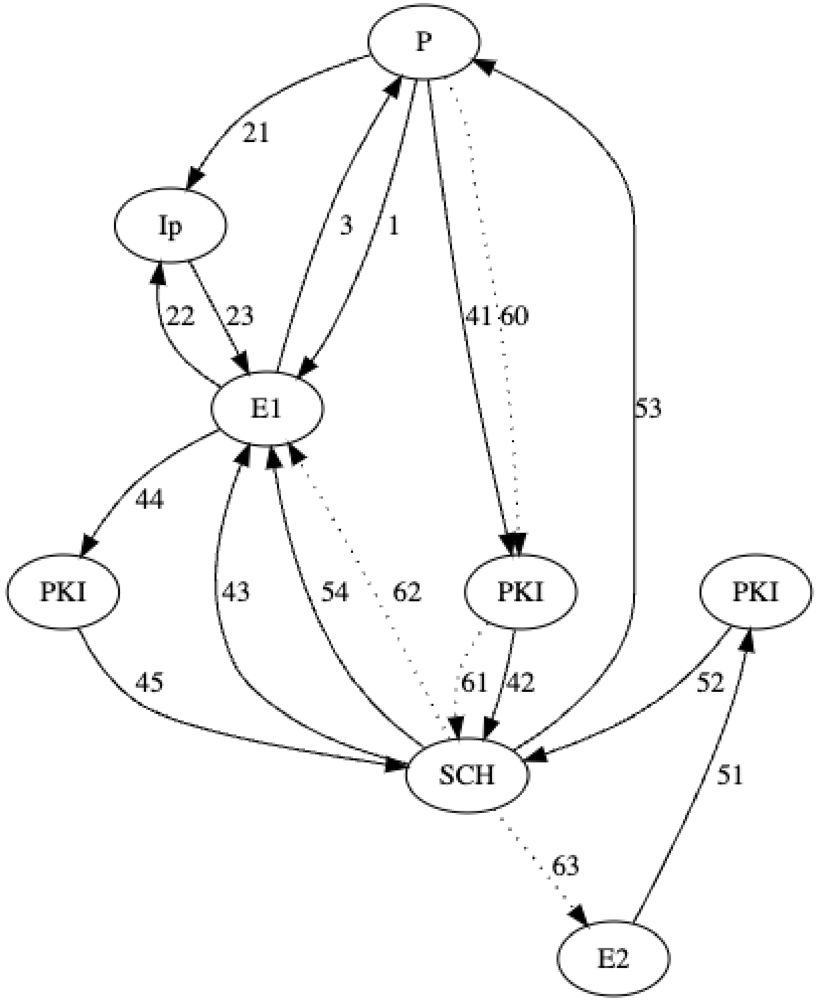
5. Upon E_2 accessing P's message, SCH notifies both P and E_1.

6. SCH may be designed to allow P to withdraw or revoke P’s consent.



Procedure Enabled by PKI and SCH

- Application in Medical Services
  - P: Patient
  - I_P: Patient's biopsy sample
  - E_1: Hospital/Clinic
  - E_2: Biopsy Analysis Company



Scenario Reflecting Physician-Hospital Relationships

- In healthcare, individual physicians (or other healthcare professionals) directly interact with patients.
- It is crucial to verify:
  - The identity of each physician
  - The validity of their qualifications
  - The healthcare institution they are affiliated with

Scenario Reflecting Physician-Hospital Relationships

- Actors:
  - P: Patient
  - H_1: Hospital/Clinic providing care to P
  - Ph_1: P's primary physician (affiliated with H_1)
  - H_2: Another Hospital/Clinic
  - Ph_2: A physician (affiliated with H_2)

Scenario Reflecting Physician-Hospital Relationships

- The roles of PKI:
  - **Authenticate:** The identities of P, H_1, Ph_1, H_2, and Ph_2.
  - **Certify:** Multiple factors for Ph_1 & Ph_2 (legal medical institutions, public health insurance coverage).
  - **Verify:** Ph_1 & Ph_2 as licensed physicians, affiliated with their respective institutions.
  - **Authenticate messages**:
    - From/to Ph_1 (acting on behalf of H_1).
    - From/to Ph_2 (acting on behalf of H_2).

Scenario Reflecting Physician-Hospital Relationships

1. P provides informed consent to Ph$_1$, acting on behalf of H$_1$, to obtain I$_P$.

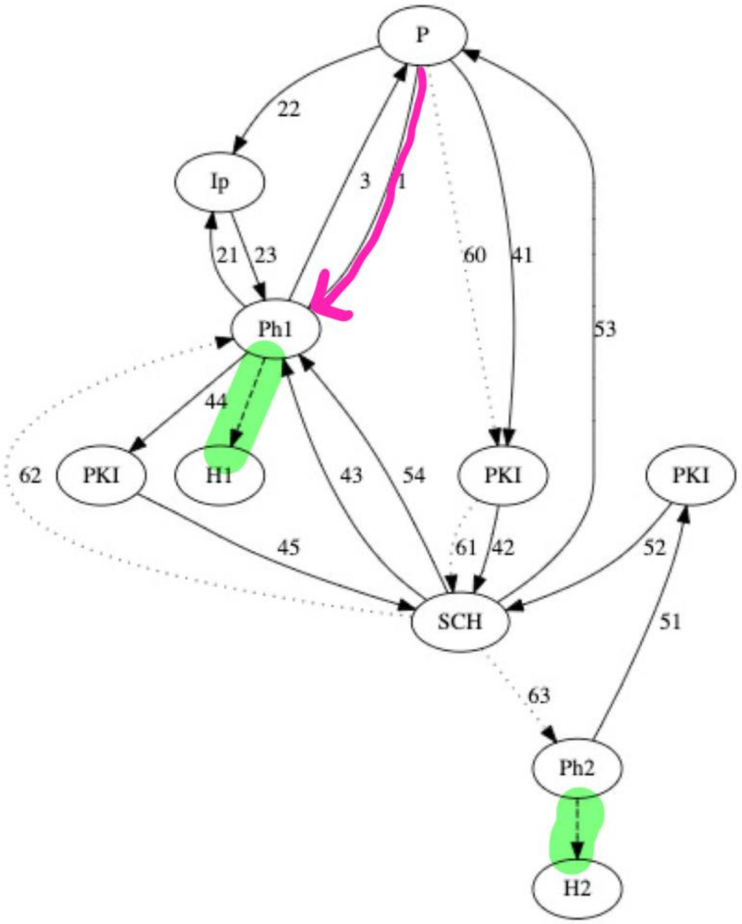
2. Ph$_1$, acting on behalf of H$_1$, obtains I$_P$.

3. Ph$_1$, acting on behalf of H$_1$, informs P of Ph$_1$'s intention to share I$_P$ with Ph$_2$ (affiliated with H$_2$) and Ph$_2$'s medical team at H$_2$. Ph$_1$ also provides P with the identification of both Ph$_2$ and H$_2$.

4. P creates a message expressing P's consent, or revocable consent, for Ph$_2$, acting on behalf of H$_2$, to obtain I$_P$ from Ph$_1$, acting on behalf of H$_1$. Ph$_1$, acting on behalf of H$_1$, countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

5. When Ph$_2$, acting on behalf of H$_2$, accesses P's message, SCH notifies both P and Ph$_1$.

6. SCH may allow P to withdraw or revoke P's consent.



Scenario Reflecting Physician-Hospital Relationships

1. P provides informed consent to Ph_1, acting on behalf of H_1, to obtain I_P.

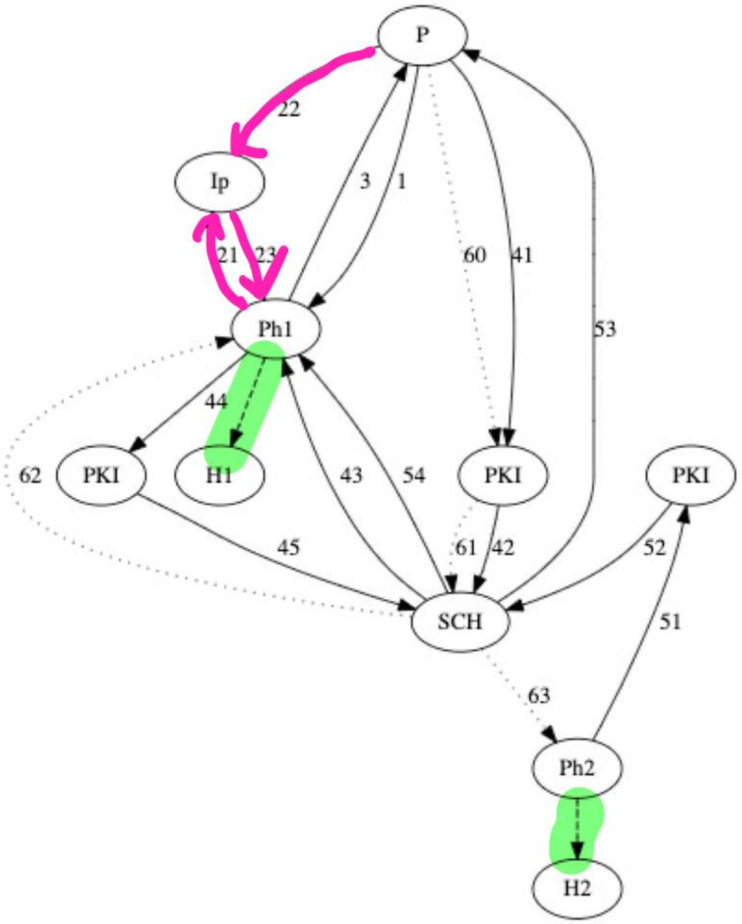
2. Ph_1, acting on behalf of H_1, obtains I_P.

3. Ph_1, acting on behalf of H_1, informs P of Ph_1’s intention to share I_P with Ph_2 (affiliated with H_2) and Ph_2’s medical team at H_2. Ph_1 also provides P with the identification of both Ph_2 and H_2.

4. P creates a message expressing P's consent, or revocable consent, for Ph_2, acting on behalf of H_2, to obtain I_P from Ph_1, acting on behalf of H_1. Ph_1, acting on behalf of H_1, countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

5. When Ph_2, acting on behalf of H_2, accesses P's message, SCH notifies both P and Ph_1.

6. SCH may allow P to withdraw or revoke P’s consent.



Scenario Reflecting Physician-Hospital Relationships

1. P provides informed consent to Ph$_1$, acting on behalf of H$_1$, to obtain I$_P$.

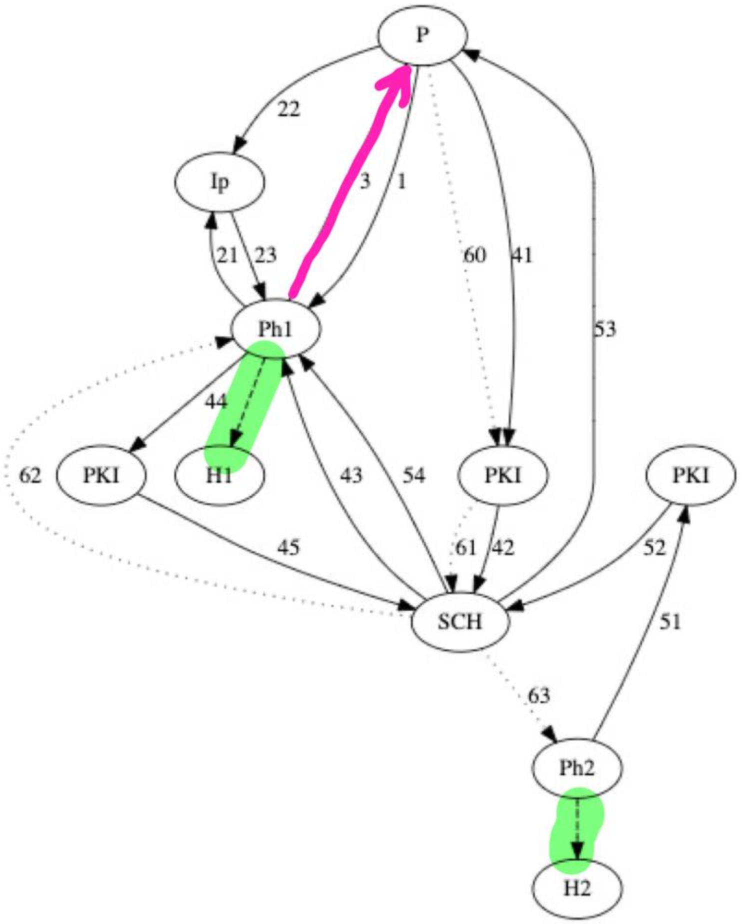
2. Ph$_1$, acting on behalf of H$_1$, obtains I$_P$.

3. Ph$_1$, acting on behalf of H$_1$, informs P of Ph$_1$'s intention to share I$_P$ with Ph$_2$ (affiliated with H$_2$) and Ph$_2$'s medical team at H$_2$. Ph$_1$ also provides P with the identification of both Ph$_2$ and H$_2$.

4. P creates a message expressing P's consent, or revocable consent, for Ph$_2$, acting on behalf of H$_2$, to obtain I$_P$ from Ph$_1$, acting on behalf of H$_1$. Ph$_1$, acting on behalf of H$_1$, countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

5. When Ph$_2$, acting on behalf of H$_2$, accesses P's message, SCH notifies both P and Ph$_1$.

6. SCH may allow P to withdraw or revoke P's consent.



Scenario Reflecting Physician-Hospital Relationships

1. P provides informed consent to Ph_1, acting on behalf of H_1, to obtain I_P.

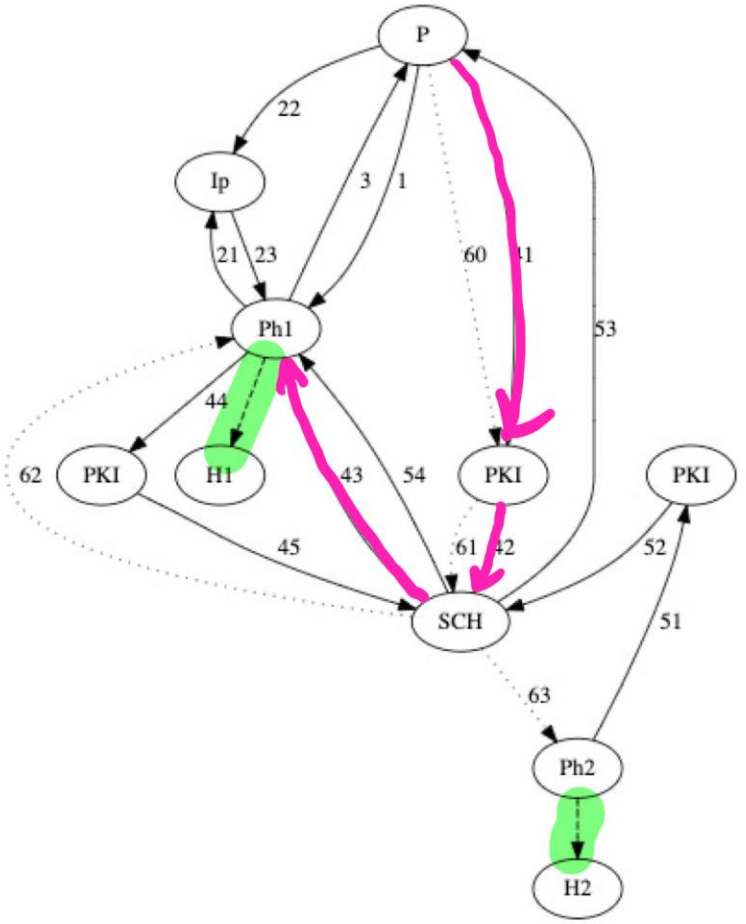
2. Ph_1, acting on behalf of H_1, obtains I_P.

3. Ph_1, acting on behalf of H_1, informs P of Ph_1’s intention to share I_P with Ph_2 (affiliated with H_2) and Ph_2’s medical team at H_2. Ph_1 also provides P with the identification of both Ph_2 and H_2.

4. P creates a message expressing P's consent, or revocable consent, for Ph_2, acting on behalf of H_2, to obtain I_P from Ph_1, acting on behalf of H_1. Ph_1, acting on behalf of H_1, countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

5. When Ph_2, acting on behalf of H_2, accesses P's message, SCH notifies both P and Ph_1.

6. SCH may allow P to withdraw or revoke P’s consent.



Scenario Reflecting Physician-Hospital Relationships

1. P provides informed consent to Ph$_1$, acting on behalf of H$_1$, to obtain I$_P$.

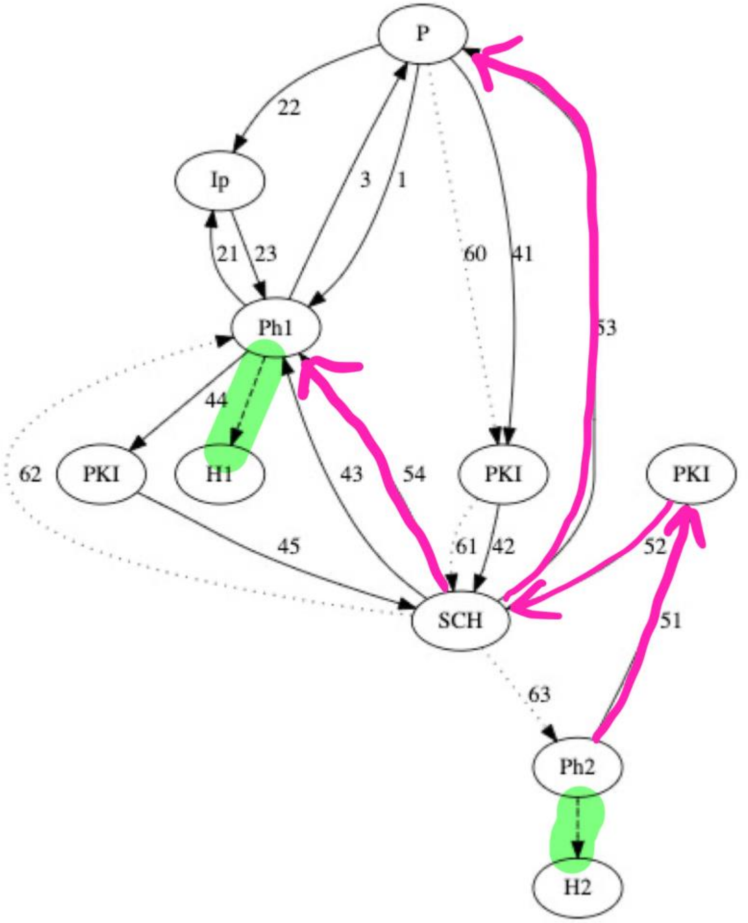
2. Ph$_1$, acting on behalf of H$_1$, obtains I$_P$.

3. Ph$_1$, acting on behalf of H$_1$, informs P of Ph$_1$'s intention to share I$_P$ with Ph$_2$ (affiliated with H$_2$) and Ph$_2$'s medical team at H$_2$. Ph$_1$ also provides P with the identification of both Ph$_2$ and H$_2$.

4. P creates a message expressing P's consent, or revocable consent, for Ph$_2$, acting on behalf of H$_2$, to obtain I$_P$ from Ph$_1$, acting on behalf of H$_1$. Ph$_1$, acting on behalf of H$_1$, countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

5. When Ph$_2$, acting on behalf of H$_2$, accesses P's message, SCH notifies both P and Ph$_1$.

6. SCH may allow P to withdraw or revoke P's consent.



Scenario Reflecting Physician-Hospital Relationships

1. P provides informed consent to Ph_1, acting on behalf of H_1, to obtain I_P.

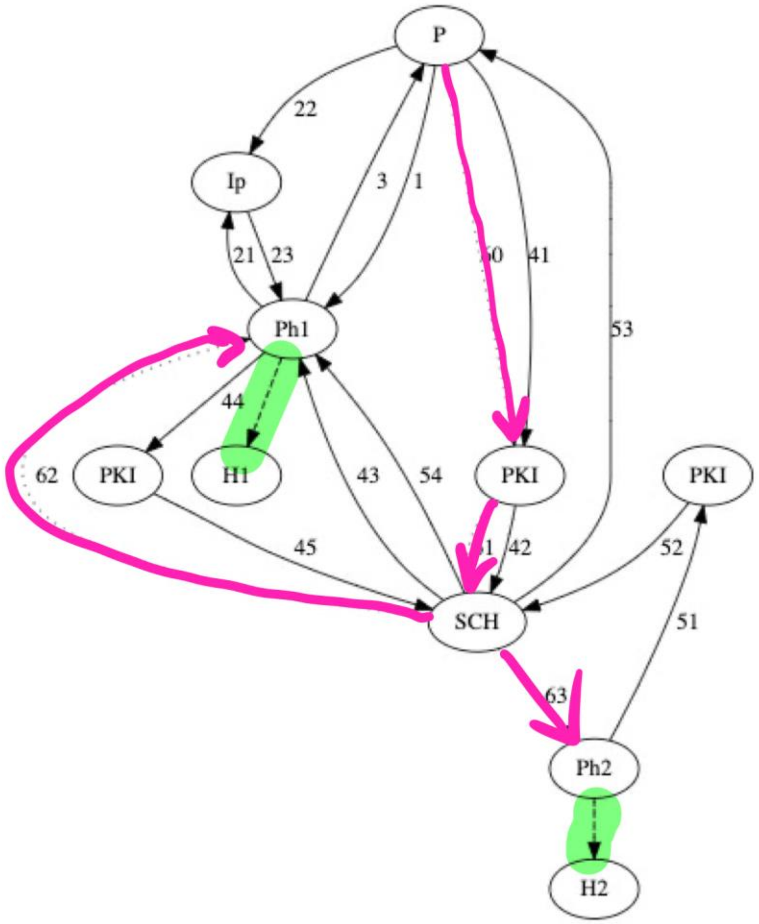
2. Ph_1, acting on behalf of H_1, obtains I_P.

3. Ph_1, acting on behalf of H_1, informs P of Ph_1's intention to share I_P with Ph_2 (affiliated with H_2) and Ph_2's medical team at H_2. Ph_1 also provides P with the identification of both Ph_2 and H_2.

4. P creates a message expressing P's consent, or revocable consent, for Ph_2, acting on behalf of H_2, to obtain I_P from Ph_1, acting on behalf of H_1. Ph_1, acting on behalf of H_1, countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

5. When Ph_2, acting on behalf of H_2, accesses P's message, SCH notifies both P and Ph_1.

6. SCH may allow P to withdraw or revoke P's consent.



Scenario Reflecting Physician-Hospital Relationships

1. P provides informed consent to Ph$_1$, acting on behalf of H$_1$, to obtain I$_P$.

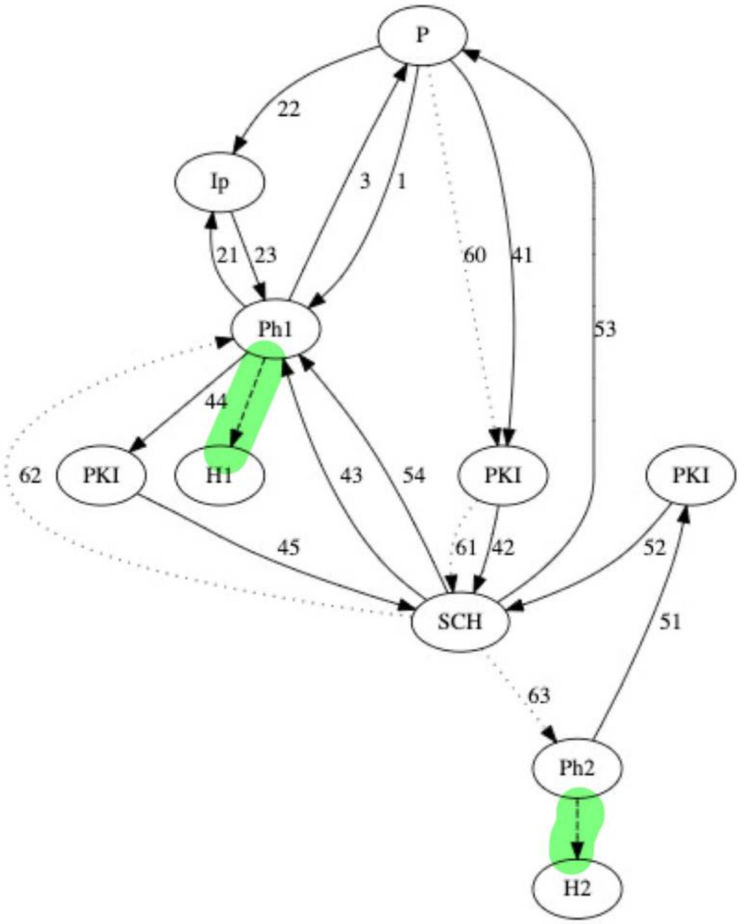
2. Ph$_1$, acting on behalf of H$_1$, obtains I$_P$.

3. Ph$_1$, acting on behalf of H$_1$, informs P of Ph$_1$’s intention to share I$_P$ with Ph$_2$ (affiliated with H$_2$) and Ph$_2$’s medical team at H$_2$. Ph$_1$ also provides P with the identification of both Ph$_2$ and H$_2$.

4. P creates a message expressing P's consent, or revocable consent, for Ph$_2$, acting on behalf of H$_2$, to obtain I$_P$ from Ph$_1$, acting on behalf of H$_1$. Ph$_1$, acting on behalf of H$_1$, countersigns this message. The message and the countersignature are then authenticated by PKI and deposited with SCH.

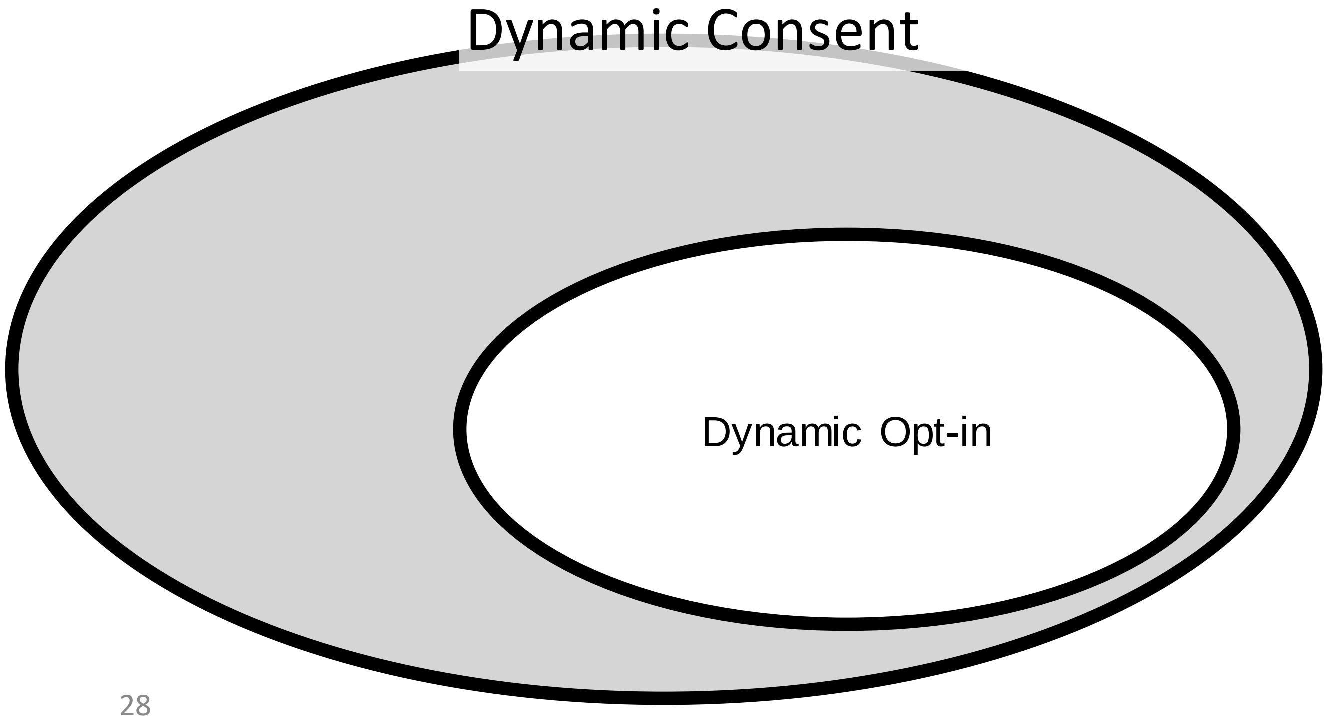
5. When Ph$_2$, acting on behalf of H$_2$, accesses P's message, SCH notifies both P and Ph$_1$.

6. SCH may allow P to withdraw or revoke P’s consent.



Conclusion: Overcoming Challenges and Promoting Medical and Healthcare Data Sharing

- The proposed scheme facilitates the social implementation of Dynamic Consent.
- The proposed scheme can be called "Dynamic Opt-in" as a subset of dynamic consent.
  - “Dynamic Opt-in” Trademark Registration No. 6724488 (Japan), right holder: Japan Communications Inc.



Conclusion: Overcoming Challenges and Promoting Medical and Healthcare Data Sharing

- Personal information protection laws pose challenges to medical and healthcare data sharing.

- Changes in laws within a single jurisdiction do not eliminate obstacles to cross-border data sharing.

- Facilitating dynamic and rapid acquisition of informed consent through PKI and SCH could be a key to solving this problem.