Part 2 - Common Data Requirements (PII, PHI, PFI) Across HIPAA, HITRUST, SOC 2, GLBA

(Fully tailored to the Secure Hospital Patient Management & Billing System)

---

1. Common Data Fields Identified

The following PII, PHI, and PFI fields appear **consistently** across all four frameworks:

A. Personal Identifiable Information (PII)

1. **Full Name**
2. **Date of Birth**
3. **Home Address**
4. **Phone Number**
5. **Email Address**
6. **National Identification Number (SSN or equivalent)**
7. **Gender**
8. **Emergency Contact Information**
9. **IP Address / Device ID (when using patient portals)**

B. Protected Health Information (PHI)

(HIPAA & HITRUST-specific)

10. **Medical Record Number (MRN)**
11. **Diagnosis Information**
12. **Prescriptions / Medication Info**
13. **Treatment History**
14. **Doctor’s Notes / Clinical Observations**
15. **Insurance Policy Number**
16. **Healthcare Provider Information**

C. Protected Financial Information (PFI)

(GLBA + SOC 2)

17. **Credit Card Number**
18. **Bank Account Number**
19. **Billing Address**
20. **Invoice History**
21. **Payment Transaction IDs**

These 21 fields together cover all mandatory sensitive information required by healthcare and financial compliance frameworks.

---

2. Grouping of Data Fields (With Justification)

Below is the **correctly grouped structure**, which matches real-world healthcare security standards.

Group 1 — Identity & Demographic Information (PII)

Fields:

- Full Name
- Date of Birth
- Gender
- Address
- Phone
- Email
- Emergency Contacts
- SSN
- IP/Device ID

Justification:

These fields uniquely identify a patient and are protected across **HIPAA, SOC 2, HITRUST, and GLBA** because unauthorized disclosure can cause identity theft, fraud, impersonation, and privacy violations.

Group 2 — Medical / Clinical Information (PHI)

Fields:

- Medical Record Number (MRN)
- Diagnosis information
- Treatment history
- Prescription details
- Physician notes
- Insurance policy number

Justification:

HIPAA and HITRUST consider these as **PHI**, the most sensitive category.

The exposure of diagnoses, medications, or treatment history can cause discrimination, emotional harm, and severe privacy risk.

MRN and insurance details also tie the patient to specific medical activities.

Group 3 — Financial & Billing Information (PFI)

Fields:

- Credit card number
- Bank account number
- Billing address
- Invoice history
- Payment transaction IDs

Justification:

GLBA mandates strong protection for customer financial data (NPI — Nonpublic Personal Information).

Storing payment data requires encryption, strict access controls, and auditing because disclosure can cause direct financial theft and fraud.

Group 4 — System & Audit Information (PII + Operational Data)

Fields:

- Login username
- Hashed password
- User role (Doctor, Admin, Nurse, Billing Agent)

- Timestamp logs
- IP address of access
- Session IDs

Justification:

SOC 2 and HITRUST emphasize access control, audit trails, and operational security.

These data points ensure accountability, traceability, and detection of unauthorized activity.

---

3. Why These Fields Are Common Across All Compliance Frameworks

HIPAA & HITRUST

Protect health, identity, and insurance-related information.

All PHI and PII fields fall under HIPAA's 18 PHI identifiers.

GLBA

Protects financial + personal information used in billing and payments.

Covers PFI + some PII fields (SSN, address, financial accounts).

SOC 2

Focuses on:

- Access controls
- Privacy
- Confidentiality
- Security of customer data

SOC 2 applies to **all PII, PHI, and PFI fields** since all are stored in a cloud or software system.

Because your system handles **medical + personal + financial data**, it overlaps all four frameworks, making your data classification strong and legitimate.