UNNUS · HEALTHCARE DESIGN STUDIO

The patient-data journey worksheet

Choose one real website form. Follow a test submission from the patient's screen to every vendor, inbox, database, log, backup, export, and human hand. If the route becomes vague, stop and investigate.

1. Name the journey

PAGE / FORM URL

WORKFLOW OWNER

PURPOSE OF COLLECTION

LAST REVIEWED

2. Draw the route

Patient enters
List every field, free-text box, file, cookie, identifier, and page context.

→

Systems process
Form, CMS, API, email, CRM, scheduler, analytics, logs, backups.

→

People access
Front desk, clinicians, agency, IT, support, vendors, developers.

3. Record the data

IDENTITY FIELDS

HEALTH / APPOINTMENT CONTEXT

TECHNICAL IDENTIFIERS

WHAT CAN BE REMOVED?

4. Mark every destination

System / vendor	Data received	Why needed	BAA / contract checked?	Retention / deletion

Do not stop at the database. Check email notifications, application logs, analytics events, support tools, screenshots, spreadsheets, backups, staging, and local downloads.

UNNUS · HEALTHCARE DESIGN STUDIO

The questions that expose the gaps

A checkbox is not proof. For every “yes,” name the owner, system, contract, configuration, or test that supports it.

Forms and flows

- ☐ We collect only what this step genuinely needs.
- ☐ Sensitive free text is avoided or handled appropriately.
- ☐ Names, conditions, and appointment details stay out of URLs.
- ☐ Confirmation pages and emails reveal no unnecessary details.
- ☐ Urgent and emergency limitations are clear.
- ☐ Sensitive intake lives in an appropriate secured workflow.

Invisible witnesses

- ☐ We inspected network requests on the form and confirmation pages.
- ☐ Analytics events contain no sensitive values or revealing context.
- ☐ Pixels, tag managers, chat, call tracking, replay, and embeds were reviewed.
- ☐ Each third-party script has an owner and a current purpose.
- ☐ Consent behavior is configured and tested.
- ☐ Sensitive payloads are excluded from logs and error tools.

Vendors, people, and custody

- ☐ We know which vendors create, receive, maintain, or transmit PHI.
- ☐ Required BAAs match the products and plan actually used.
- ☐ Staff have individual accounts and appropriate MFA.
- ☐ Access follows least privilege and is reviewed.
- ☐ Backups, exports, staging, tickets, and screenshots are in the map.
- ☐ Departed staff, vendors, plugins, and integrations lose access.
- ☐ Retention and deletion are documented.
- ☐ An incident has a named response owner.

Turn findings into work

Risk / unanswered question	Owner	Due date

Next step: run the public website through the free HIPAA risk scanner, compare its findings with this map, then review the full workflow with qualified privacy, security, and legal professionals.

This worksheet is educational. It does not determine whether HIPAA applies to an organization, perform a formal risk analysis, provide legal advice, or certify compliance.