

2027-04-27 · 80 minutes

Privacy check

Your goal: Review your public health product for privacy and data-protection concerns.

One product: Privacy audit listing collected data, identifiable items flagged for de-identification, access rules, and a 3-5 sentence privacy statement.

Question: What does a useful public-health product really need to know about a person?

Start the work

A usable message names its audience, preserves the evidence and gives a realistic action; plain wording alone does not prove behavior change.

1. List any personal or health data your product collects or displays.
2. Identify which items could identify an individual.
3. Decide what data can be removed or aggregated.
4. Note who should and should not have access.
5. Write a short privacy statement for your product.

If access or the assignment is unavailable, save the dated work and mark submission and portfolio attachment pending. Follow teacher identity and filename instructions locally.

Words you will use

privacy

Appropriate control over access to personal information.

privacy audit

A review of information collection, use, sharing and related risks.

data

Recorded information.

personal data

Information about a person that may identify or be linked to them.

health data

Information about health, care or test results.

identifiable

Able to point to an individual, directly or through a combination of information.

direct identifier

A detail, such as a name, that directly points toward a person.

indirect identifier

A detail that may identify someone when combined with other information.

re-identification

Linking information back to a person whose identity had been removed or obscured.

name-free

Lacking a person's name; this alone does not mean anonymous.

anonymous

Not reasonably linkable to an individual in the relevant setting; not a label this exercise can certify.

de-identification

Reducing identifying information using a defined process; a legal standard may impose specific requirements.

aggregation

Combining individual records into group summaries.

coarsening

Replacing detailed values with broader categories.

suppression

Withholding a value or record from a release.

small cell

A table entry representing a small group or count.

threshold

A cutoff used in a stated decision rule.

k

The proposed number of people sharing a disclosed combination of features; its adequacy depends on context.

outside information

Information beyond the released table that someone could use to make a link.

differencing

Subtracting related published values to infer another value.

inventory

A complete list of the information a design touches.

collection

Obtaining or recording information.

display

Information shown to a viewer.

storage

Keeping information for later use.

free text

An open response field where people can type unstructured words.

log

A technical record of activity or events.

IP address

A network address that may help link activity to a device, connection or user.

session code

An identifier used to connect activity within or across visits.

cookie

Information stored by a website in a browser, potentially used to link visits.

access rule

A statement of who may use information and what they may do.

least privilege

Giving each role only the access needed for its task.

role

A defined set of responsibilities.

vendor

An outside provider of a service.

export

A copy of information taken out of its original system.

retention

How long information is kept and for what reason.

disposal

Removal of information when it is no longer needed, using an appropriate method.

permission

Agreement allowing a specified action; it does not by itself settle every legal or privacy issue.

consent

A person's informed agreement to a stated action.

authorization

Formal permission under a relevant rule or process.

HIPAA

The Health Insurance Portability and Accountability Act, a US law with defined health-information rules.

covered entity

A health plan, clearinghouse or qualifying healthcare provider covered by HIPAA rules.

business associate

A service provider handling protected health information for a covered entity in a defined role.

Safe Harbor

A HIPAA de-identification method with specified identifier-removal and knowledge requirements.

Expert Determination

A HIPAA method in which a qualified expert documents that identification risk is very small.

compliance

Meeting the requirements of an applicable rule; not established by this paper exercise.

privacy statement

A short explanation of a product's information practices.

tuberculosis (TB)

A disease caused by bacteria; the example supplies no actual test or diagnosis.

mutually exclusive

Groups that do not overlap.

exhaustive

Groups that together include every item in the stated total.

wireframe

A rough layout showing a product's parts.

usability

How readily intended users can use a product.

portfolio

An organized collection of work and evidence.

prototype

An early model of a proposed product.

proposed

Suggested but not yet implemented.

risk

The chance of a specified harmful outcome under stated conditions.

H1: audit a design, not a person

Use your own public-health draft if you have a teacher-approved, nonidentifying copy. If it is missing or contains private records, use the complete fictional design D1. Do not copy real names, addresses, contact details or health histories into this exercise.

D1 is an unbuilt paper sketch. It has collected nothing. Describe what its proposed features would collect or display. Your completed audit is original practice; it does not prove that you reviewed or changed a real product.

First name one category of health information a fictional person might want kept private. Do not disclose anything about yourself or a classmate. Then inventory D1 and flag combinations that could identify someone.

The prior message lesson taught that a usable message needs an audience, evidence and a realistic action. Preserve those useful functions while questioning whether any personal data is needed.

D1: complete fictional product specification

Original design: Flu Information Board, a paper sketch for adults seeking public guidance and questions to ask a provider. Its main purpose is to display a general message and public source links. It does not book care or provide diagnosis.

The initial proposal adds a feedback form and a small-area dashboard. Those features are not required to read the message. No form, website, database or tracking service has been built or connected.

D1a: full name, entered in the form and saved in a response table; not shown on the dashboard. D1b: email address, entered and saved for proposed follow-up; not publicly shown.

D1c: exact age, entered and saved, then displayed in each dashboard record. D1d: street address, entered and saved; the dashboard shows a small attendance area derived from it.

D1e: test-result category, entered and saved, then displayed in each dashboard record. D1f: optional free-text comment, saved and displayed exactly as written, with no review.

D1g: submission date and time, automatically saved and displayed. D1h: IP address, automatically saved in hosting logs; not displayed on the dashboard.

D1i: session code, automatically saved with the response and in a cookie. It could connect repeated visits; it is not a person's name. D1j: feedback-topic choice, saved with the response but displayed only as a total by topic.

All ten fields are proposed inputs, not actual records. The suggested topics are source link, wording, and access question. No submitted values, contact addresses or personal test results are supplied.

Proposed access: any public viewer sees the dashboard records and topic totals. Every project teammate can edit the response table. A teacher reviewer receives a full export. A hosting vendor can access technical logs. No deletion date or access review is defined.

For revision, you may remove the feedback form and dashboard entirely. Or propose only the minimum fields needed for a justified feature, with restricted access and an explicit review plan. Do not claim an unbuilt control works. Explain any useful function lost when data are removed.

E1: identification and small groups

A name directly points toward a person. Other details may identify someone when combined with outside information. Exact age, a small place, a date or an unusual health detail can narrow the possibilities. A name-free code can still link records.

HHS describes two HIPAA de-identification routes: Safe Harbor and Expert Determination. They have specific requirements. Deleting only a name is not either complete process. Even properly de-identified data retain some identification risk. [HHS-ID]

Aggregation combines records into group summaries. Coarsening replaces detail with broader categories. Suppression withholds a value or record. These can reduce risk, but no universal group size guarantees privacy. HHS does not prescribe one universal k value. [HHS-ID]

A total can also reveal a hidden small value by subtraction. Review all related releases, not just one cell. A proposed threshold is a rule to test against the whole design and outside knowledge, not a certificate of anonymity.

E2: collect less and control access

FTC advises organizations to inventory personal information, collect only what they need, limit access and dispose of data they no longer need. It calls limiting access to a person's job needs the principle of least privilege. [FTC]

Inventory displayed fields and hidden storage or logs. A field can create risk even when it is not public. A free-text box can receive names or health details that its label did not request.

For each retained item, specify the purpose, who may use it, what they may do and who must not receive it. State a review or deletion rule as a proposal. No retention period is supplied as school policy here.

Public source links can be useful without a person-level response table. Removing unnecessary collection can be a better choice than gathering details and trying to anonymize them later. A checkbox does not make an unnecessary disclosure harmless.

E3: law and an honest privacy statement

HIPAA rules apply to defined covered entities and business associates. They do not automatically cover every health-related classroom product or app. Other duties may apply; this exercise does not decide legal coverage. [HHS-SCOPE]

HIPAA permits some uses and disclosures under specified conditions without individual authorization. Do not replace that rule with “all health information always needs consent under HIPAA.” Permission, legal authority and good privacy design are related but different questions. [HHS-RULE]

Write three to five sentences describing the revised design: its purpose and collection, any sharing or display, permitted access, and the retention/review plan. Say when a feature has been removed. Use proposed or future wording for changes not implemented.

Match every statement to your audit. Do not promise “anonymous,” “HIPAA compliant” or “nothing is tracked” without evidence. If a technical setting or service practice is unknown, identify the check needed before a real release.

Q1: self-check without real records

Original hypothetical dashboard card: age 16, fictional District F attendance area, and a positive tuberculosis test category. No actual person or test exists. Tuberculosis, or TB, is a bacterial disease. This is a privacy example, not a diagnosis. [CDC-TB]

The name is absent. Explain why protection is not established, what outside knowledge could raise risk, and what you would remove, combine or withhold. Do not try to identify a real person. A wider group may reduce risk without proving safety.

For a restart, begin with the fields a viewer sees. Then add stored fields and logs from D1. Resume the first unfinished step: inventory, identification flags, removal/aggregation, access rules or statement.

If stuck, compare just exact age and small area. Describe why their combination may narrow a group, propose a change, then return to all ten fields and the full product.

For a solo check, compare each sentence of your privacy statement with the inventory and access table. Flag any promise that the design does not support. Record one revision or a justified confirmation. A real peer may do the same check; do not invent their reply.

X1: optional threshold stress test

Use these original invented counts only for the extension. A proposed table has two mutually exclusive, exhaustive groups: Group A has fewer than 5 responses; Group B has 8; the total is 10. No people or responses were observed.

A designer proposes hiding cells below 5. They hide A but publish $B = 8$ and the total = 10. Show the subtraction that reveals A. This exposes a count in the toy example; it does not identify an actual person.

Design a different name-free example using invented category labels and counts. State a minimum-group rule and test it against combinations and related totals. Then change the release, such as withholding a second value or not publishing the table.

Explain what your rule fixes and what remains unknown. Hiding a small count or setting $k = 5$ alone does not guarantee anonymity or establish HIPAA compliance.

P1: actual work and next steps

For April 27, save your Privacy check in Lab Notebooks. Your product needs the inventory, identifiable items flagged for de-identification, access rules and a three-to-five-sentence statement. Keep the actual April 26 message pending if you have not completed it.

Ask which parts of Activity 5.1.2 Public Health in the News accompany this audit. The activity requires map/video exploration, filtered observations, three current local/national/international articles and an organizer. At least one article must address a noninfectious issue.

It also requires genuine partner comparison, two national/international map flags, wall-map work, class reflection and assigned conclusions. The map supports a later 5.1.3 grant proposal. This paper audit supplies none of those actual performances or current articles.

Confirm the assigned materials and stopping point. Keep the five conclusion topics separate: malaria and two risk-reduction strategies, disease/risk-factor distribution, vaccination barriers and a strategy, chronic/infectious patterns, and a priority concern.

After genuine assigned work, add the privacy statement and access rules to the required Problem 5 evidence portfolio. Do not mark the activity, portfolio attachment or peer exchange complete merely because you finished D1 practice.

Keep your message, audience information, privacy review and later usability revision with the weekly public-health product. The required slide/paper wireframe is separate. The next dated submission is Thursday, April 29, in Lab Reports.

Before April 29, build your wireframe in Lab Notebooks (about 25 minutes). No homework is due before this class. April 28 is a catch-up day. Confirm the product submission deadline with your teacher.

Ask your teacher how much home work to plan, and do not mark the wireframe preparation complete until you have done it.

Do not replace today's privacy check with a different task on your own.

Save one PDF in your enrolled BI section under the assignment matching Privacy check. Follow teacher filename and identity instructions locally. If access or the assignment is missing, save the dated work and mark submission pending.

Any real product, technical collection settings, permissions and legal review require responsible confirmation before public use. This class exercise authorizes no real collection, disclosure, data deletion or campaign launch.

M1: a different complete leaflet audit

Original model: a printed water-safety resource leaflet for fictional library visitors. The proposed sign-in sheet asks for a visitor's name, home address and reason for requesting a leaflet. A separate counter records only the number of leaflets taken each day.

My inventory has four items. Name is directly identifying. Address can identify a household. The free-text reason could reveal health details. A daily leaflet count has no individual row, but a very small count with outside knowledge could still be revealing.

My revision removes the sign-in sheet and free-text reason. The purpose is to share public resources, not contact visitors. I keep a private total for supply planning, without dates in the published material. This reduces detail but sacrifices daily demand analysis.

My proposed access rule lets one supply coordinator see and update the count. The public sees the leaflet and source links only. Other volunteers do not receive the count. The coordinator reviews whether to keep the count after the supply decision; no school retention policy is asserted.

My four-sentence statement: This proposed leaflet offers public resource information without a sign-in sheet. A supply coordinator would record only an undated total of leaflets taken for ordering. Only that coordinator would use the total, and it would not be published. The coordinator would review and discard it after the supply decision if no applicable retention duty requires keeping it.

My check finds that the statement matches the revised inventory and roles. Before real use, the responsible owner would confirm retention duties and the counting method. This is a distinct invented model, not your Flu Information Board answer or a completed service change.

Try the decision

Which revision best fits D1's information purpose and the evidence?

- Remove unnecessary collection, justify anything retained, restrict access and label controls as proposed until checked.
- Delete names, keep all other fields and publish the dashboard as anonymous.
- Publish every group with at least five records and promise that no one can be identified.

Explain your choice using the reading. Discuss it or say it to yourself. This practice does not add another submission.

Your 80-minute flow

0–5 minutes	Attempt the category warmup, screen inventory and combination flag.
5–20 minutes	Read D1/E1 and list all ten proposed fields, including hidden storage.
20–40 minutes	Evaluate identification risk; decide what to remove, combine or retain and complete Q1.
40–55 minutes	Define allowed and denied access for the revised design.
55–70 minutes	Write the three-to-five-sentence statement and compare it with the audit.
70–80 minutes	Complete a solo or actual peer check, revise, and name one change and its tradeoff.

Your response record

Use these labels on paper or in your document. The space below also works when this page is printed.

Category, screen inventory and combinations

Name one health-information category a fictional person might want kept private. List what D1 would display, and flag a combination that could identify someone.

Use categories only. Do not disclose your own information or name a real person.

Use this space or the same labeled section in your existing document. Add paper when your table, graph or drawing needs more room.

All ten proposed fields

Inventory D1a through D1j. For each, record collection/storage/display, identifying risk, purpose and your remove/aggregate/retain decision with a reason.

Include hidden logs and codes. No field has collected actual data. You may remove unnecessary features instead of collecting details first.

Use this space or the same labeled section in your existing document. Add paper when your table, graph or drawing needs more room.

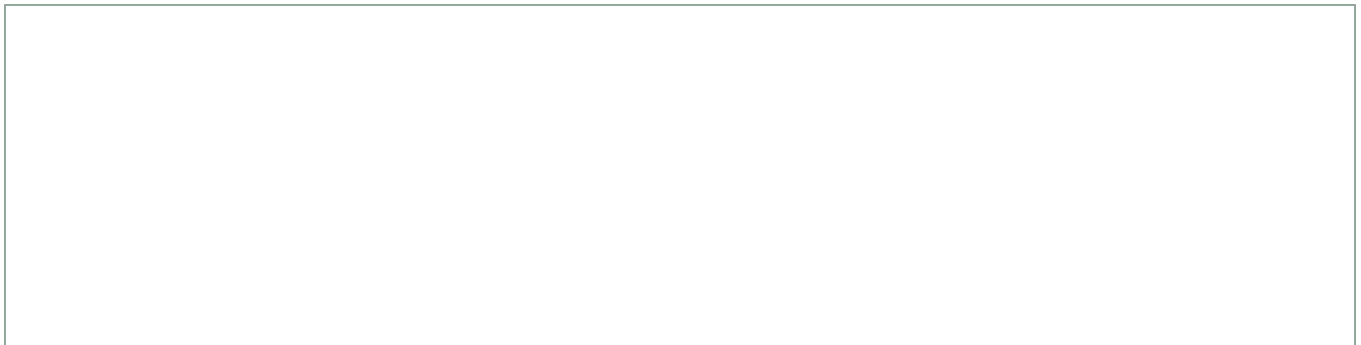


Name-free self-check

Complete Q1. Explain what the hypothetical card cannot establish about privacy, one possible outside-information link, and a bounded change.

Do not identify a real person or promise that a larger group guarantees safety. Use E1.

Use this space or the same labeled section in your existing document. Add paper when your table, graph or drawing needs more room.



Access rules for the revised product

Write rules for public viewers, teammates, teacher reviewer, hosting vendor and the responsible owner. State permitted information/action, denied access and any verification needed.

Use your revised field decisions. If you remove a feature or need no hosting, say so rather than inventing retained data or a vendor contract.

Use this space or the same labeled section in your existing document. Add paper when your table, graph or drawing needs more room.

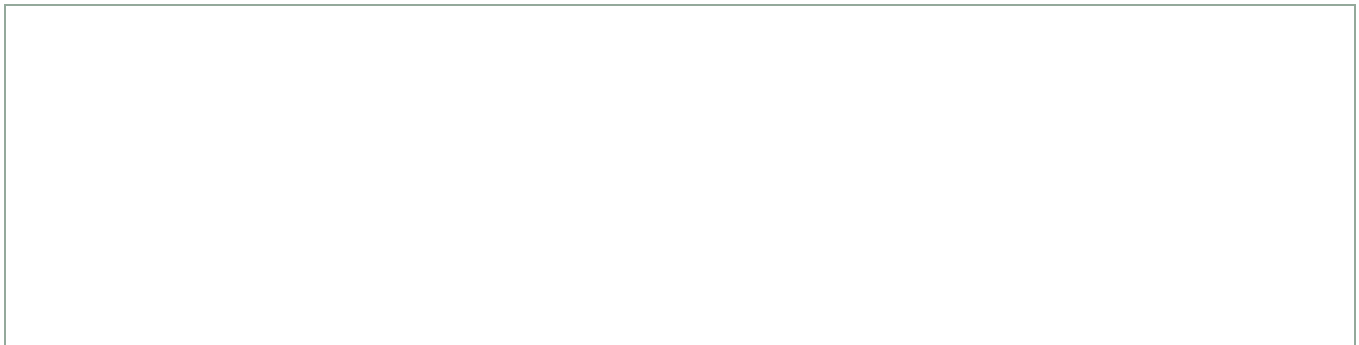


Three-to-five-sentence privacy statement

Write a statement matching your revised design. Include purpose/collection, sharing/display, permitted access and retention or review. Label unimplemented changes as proposed.

E3 supplies the structure; M1 is a different model. Do not claim guaranteed anonymity or legal compliance.

Use this space or the same labeled section in your existing document. Add paper when your table, graph or drawing needs more room.



Solo or actual peer check

Check each statement sentence against your inventory and access rules. Record one unsupported promise and a revision, or justify confirmation.

Use Q1's complete solo check when no partner is available. Label the route and do not invent another person's feedback.

Use this space or the same labeled section in your existing document. Add paper when your table, graph or drawing needs more room.

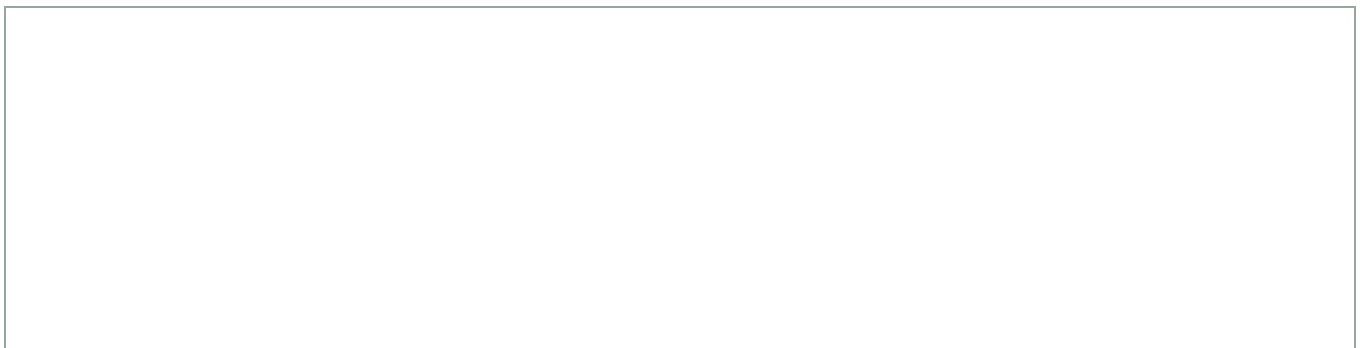


Optional threshold stress test

Use X1 to calculate the hidden count, then create a different invented name-free example. State a group-size rule, test related totals and improve the release.

Explain the remaining limit. No universal k or subtraction test guarantees privacy. Do not create real personal records.

Use this space or the same labeled section in your existing document. Add paper when your table, graph or drawing needs more room.



One change and genuine status

Name one specific change that reduces risk and one useful function affected. Check all four product parts, then record real product, official work, wireframe and submission status.

A completed fictional audit is not an actual product change. Keep the April 29 preparation and later submission separate.

Use this space or the same labeled section in your existing document. Add paper when your table, graph or drawing needs more room.



Check your product

- All collected or displayed information, including hidden technical records, is accounted for.
- Identifying details are flagged and changes are justified without an anonymity guarantee.
- Access rules and the three-to-five-sentence privacy statement agree with the revised design.
- Original practice, actual product changes and official/submission status are distinguished.

Keep the limit: A paper audit can identify design risks and propose changes. It cannot certify anonymity, legal compliance, deployed protection, real data deletion or actual coursework completion.

Turn in your work

Save one PDF with the data inventory, identification flags and changes, access rules and three-to-five-sentence privacy statement. Match Privacy check in your confirmed enrolled BI assignment; the dated folder is Lab Notebooks.

If access or the assignment is unavailable, save the dated work and mark submission and portfolio attachment pending. Follow teacher identity and filename instructions locally.

[Open this assignment in Schoology.](#)

Carry forward

Collect only what the purpose needs, test combinations and related releases, and describe the actual design without promising zero risk.

Carry the audited draft, access rules and proposed privacy statement into the April 29 product and wireframe check. Which part of the proposed product needs revision after your privacy check?

Sources and resources

[Open today's page](#)

HHS-ID · Guidance Regarding Methods for De-identification of Protected Health Information

HHS Office for Civil Rights

<https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification/index.html>

HHS-SCOPE · Covered Entities and Business Associates

HHS

<https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>

HHS-RULE · Summary of the HIPAA Privacy Rule

HHS

<https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

FTC · Protecting Personal Information: A Guide for Business

Federal Trade Commission

<https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>

CDC-TB · About Tuberculosis

CDC

<https://www.cdc.gov/tb/about/index.html>