eHealth Exchange™

CRISP Shared Services

Information Handling Transparency Best Practices

The following best practices and related guidance are the result of a collaborative effort between the eHealth Exchange and CRISP Shared Services.

We wanted to come together on this effort to emphasize the importance of information handling transparency and to pool our collective experience and expertise in developing resources that are applicable to any organization that is involved in the electronic sharing of health information.

The health information exchange landscape is continuing to evolve and expand at an increasingly rapid rate. Yet, those outside of this niche in which we are daily immersed generally have poor insight into the what, when, why, and with whom of health information exchange. And let's face it: This stuff is pretty complicated. Some of us store data, and some will use the data, once obtained, for secondary purposes; others do neither. Some of us are subject to HIPAA; others are not. Some of us are industry-facing; some of us are consumer facing; some are both. We differ in why data may be exchanged. We differ in the types of health information we handle. We differ in whom we share that information with and how. The list of differences goes on and on. None of us does the same thing in the same way. **So, for individuals to understand how we handle their health information, we need to tell them.**

About the Authors

The eHealth Exchange is the country's largest health information exchange and acts as a "network of networks," facilitating truly nationwide exchange through both technical connectivity and governance.

CRISP Shared Services is a non-profit support organization that provides technical infrastructure and professional services to state HIEs and health data utilities (HDUs) to allow them to achieve economies of scale, pool innovation, and implement best practices.

Both organizations have also committed to participation in the Trusted Exchange Framework and Common Agreement (TEFCA℠). The eHealth Exchange is a Designated Qualified Health Information Network (QHIN™), and CRISP is committed to being a Participant in the eHealth Exchange QHIN.

Let's *TALK* Best Practices

Transparency

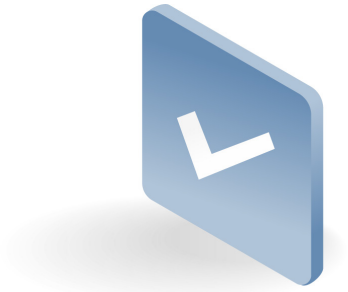
Be transparent about how you handle information.

As simple as that may sound, our review of many of the available examples that are out there suggests that it is anything but simple. We also understand the nuances and complexities of health information exchange—technical, practical, legal, etc.—and that conveying relevant information in a way that is meaningfully informative, yet straightforward and uncomplicated, is challenging. That is why we want to begin by emphasizing that step number one is simply a matter of trying. Commit to being transparent about how your organization handles individuals' information, and do your best to follow through on that commitment. Hopefully, what follows will help.

Accessibility

Make your information handling practices easy to find and identify.

One common misstep we have observed is organizations blending the concepts of information handling practices, in the context of their service or product, with their general website privacy policy (e.g., website utilization, cookies, tracking, etc.). Even if your product or service involves a web application, it is important to distinguish how information is handled through that web app (and what makes an individual subject to those information handling practices) from what information you may collect through your public-facing website. The common usage of the term "Privacy Policy" in the context of websites is why we prefer "Information Handling Practices."



Ensure this information is practically accessible.

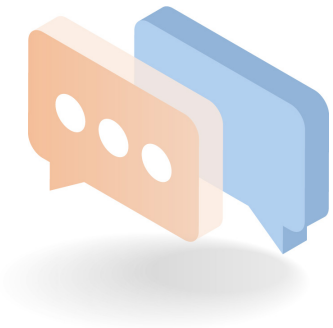
Your information handling practices should be publicly available without special effort. If you have a website, the practices should be conspicuously posted there; they should be in an obvious location, and individuals should not need to search for long to find your information handling practices. If you operate a physical location, you should post your information handling practices in a public area and/or a notice that printed copies are available (and how/where to pick one up). Any means or location of interaction with individuals whose information is impacted should be a means or location through which those individuals can obtain an explanation of your information handling practices.

Practical accessibility also involves considering different languages and formats in which to make your information handling practices available. A good starting point for this is to evaluate the demographic composition (actual or probable) of those whose information you are handling when considering issues of practical accessibility. That evaluation can assist you in identifying which formats and/or translation you should strive to make proactively available, which you should consider having readily available, and/or which you may need to address providing on an as-needed basis.

At a minimum, information handling practices that are posted on your website should meet accessible web content standards.

Language & Presentation

Use as much plain language as possible.



It can be challenging to explain concepts related to health information exchange in common, everyday terms. We are an industry that has acronyms for its acronyms, after all. Make sure to spell all of those out. If industry terminology is necessary, explain what it means. Keep sentences short. Ask someone you know who does not work in healthcare or information technology to read through your information handling practices and provide feedback. Ask them if there were any terms they did not recognize. Ask them what questions they have after reading the document. Are they able to explain back to you what they read? Before finalizing your information handling practices documentation, consider repeating this process with a group of patients and asking for their feedback.

If you find that there are certain issues that may be more nuanced and/or for which individuals may want further detail, consider addressing the main issue as concisely as possible in your main information handling practices documentation and then pointing individuals to where they can find additional information on that topic. The key is to prioritize the fundamental information. Being informative and helpful often does not mean providing everything in one place, which is a good lead-in to the next best practice...

Logically organize your information.

Logical organization involves considerations of both the internal organization of the information within the documentation and the organization of the documentation itself. For example, internal organization would include starting with an explanation of what the information is that you are handling before launching into how it is that you handle it. Broader considerations regarding the organization of your information handling practices documentation include how you organize this information across different service lines and how the information is presented across different media (e.g., on a website versus as a PDF).

A common pitfall is trying to cover too many business cases at once. Namely, it is helpful to keep information handling practices documentation across service lines separate if there are any differences in the practices that pertain to those respective service lines. Repeating information across separate documents or sections for different service lines is preferred over discussing them together and attempting to clearly identify how and when there may be differences in the information handling practices applicable to one or more particular service line(s).

Remember your audience and the purpose of providing the information.

Your information handling practices documentation is not a sales pitch. Some jargon and buzz words may be part of everyday speech, but that does not make them appropriate or useful in this context. Assume the person is reading about your information handling practices because they already have concerns about how their information is being accessed, used, or disclosed. That person is not looking for a sales pitch; they are looking to you for a straightforward explanation.

Keep it Real

Set realistic expectations.

What choices do individuals have with respect to how you handle their information? What rights do they have over how your organization handles their information? What limitations or exceptions might apply to those choices and/or rights?

There is a substantial degree of misunderstanding about whether and how health information is regulated in the United States. Many individuals are unaware, for example, that protected health information may be shared under HIPAA for Treatment, Payment, and Health Care Operations without patient consent. Many individuals are also under the mistaken impression that HIPAA protects their health information, regardless of who is in possession of that information. Health information exchange between and among HIPAA-regulated entities has predominantly taken place behind the scenes, often unbeknownst to the subject of such information. HIEs and HINs, for example, are still largely unknown to the public, and those who become aware of their existence are met with the challenge that no two are alike. One may store their data and provide direct access to it, while one merely relays the information and does not even know to whom it pertains.

As health information exchange comes increasingly into the public view, and as digital health information steadily becomes available directly to individuals on their chosen devices and through their selected applications, it is crucial that individuals are provided the resources necessary to be informed about how and when their health information is *actually* private and protected… and how and when it is not. Namely, it is important to inform individuals what control they have over the exchange of their health information and/or what rights of restriction, if any, your organization honors. Lastly, if individuals have the ability to exercise any control and/or rights over how your organization handles their health information, it is important to provide clear instructions on how individuals may go about doing so.

External Resources

U.S. Department of Justice, Civil Rights Division, Guidance on *Web Accessibility and the ADA*, available at https://www.ada.gov/resources/web-guidance/ (accessed July 24, 2023).

World Wide Web Consortium (W3C), W3C Web Accessibility Initiative (WAI) homepage, available at https://www.w3.org/WAI/ (accessed July 24, 2023).

U.S. Department of Health and Human Services, *Example of a Policy and Procedure for Providing Meaningful Communication with Persons with Limited English Proficiency*, available at https://www.hhs.gov/civil-rights/for-providers/clearance-medicare-providers/example-policy-procedure-persons-limited-english-proficiency/index.html (accessed July 24, 2023).

Plain Language Action and Information Network (PLAIN) homepage, available at https://www.plainlanguage.gov/ (accessed July 24, 2023).

Centers for Disease Control and Prevention (CDC), *Plain Language Materials and Resources*, available at https://www.cdc.gov/healthliteracy/developmaterials/plainlanguage.html (accessed July 24, 2023).

Key Questions Individuals Want Answered

What does your organization/product(s)/service(s) do?

- Avoid using jargon and buzz words, and try to think about this from the perspective of what it means for the individual and their information.
- While this should not sound like a sales pitch, it is appropriate to explain what real-world benefit(s) your organization/product(s)/service(s) provides from the standpoint of an individual whose data are implicated.

What type(s) of information about me does your organization handle?

- Be reasonably specific here, and provide examples where appropriate.
- In trying to break down the types of information, it may help to think about any information that may be mentioned later (or in other materials) as being treated differently in specific circumstances, such as limitations on the ability to opt out of having certain public health information exchanged.
- You may also want to identify types of information that your organization does not handle, and note those as exceptions.

Who is allowed to access or request my health information through [org/product/service]?

- Think about legal and business categories, and provide examples of each (e.g., Covered Entities, Business Associates, other HIEs/Networks, Apps/App developers, CBOs, etc.)
- Remember to explain "who" in plain language. For example: It may be worth mentioning that Covered Entities and Business Associates are regulated under HIPAA, but do not simply rely on the HIPAA definition to explain who/what these are. What are these in real life?

For what reasons are users allowed to access or request my health information?

- List the reasons and then provide a description of each. Again, do not simply rely on legal or contractual definitions. It might make sense to include such definitions, but then explain what they mean. Again, practical examples may be helpful.
- It may also be helpful to list certain reasons for which access to health information is not permitted and/or for which access depends upon meeting additional requirements (e.g., law enforcement with a subpoena, a family member with authorization, etc.)

Is ALL of my health information accessible to users for the reasons above? Are there any limitations?

- Connect the dots between the purposes and the people (e.g., Treatment = only healthcare providers with a treatment relationship with you).
- Explain any limitations on the type(s) of data involved (e.g., information considered "sensitive" under applicable law).
- It is also important to note limiting factors that can result in incomplete datasets.

Are users only allowed to view my information, or are they able to download, ingest, or otherwise keep a copy of my information? Once a user has a copy of my health information, what are ***they*** are allowed to do with that information?

- This is extremely important to issues of secondary use and/or redisclosure, which have significant legal and practical implications for matters such as ongoing legal protections and opt-out rights.
- If users can download or ingest information, you should explain what, if any, legal and/or contractual protections apply to the information once it is downloaded/ingested.

Do you store the information about me that is shared through [org/product/service]?

- This should provide the readers with somewhat more nuanced information about what information gets stored and for how long.
- For example, even if your organization does not store health information: how long does health information persist in your environment, and how/why might it be accessible to those within your organization; are patient demographics subject to different retention policies and, if so, why (e.g., in an MPI or in audit logs)?
- At what point / After how long is information deleted/purged?

[*If the organization persistently stores information:*] What do ***you*** do with my information once you have it? Are you allowed to use it for other purposes?

- This gets to a different issue than those above with respect to users and/or exchange purposes. This is intended to address what the organization, itself, does with the information it stores (e.g., data aggregation, reporting and analytics, etc.). This should be reasonably specific and, when possible, it is helpful to provide examples.

Do you now, or will you ever, sell my information and/or use my information for marketing purposes?

- This answer should start with either a "Yes" or a "No" and elaborate accordingly from there.

Are any of your users allowed to sell my information and/or use my information for marketing purposes?

- Are your users/customers subject to limitations on the sale and/or marketing use of data obtained through your org/service/product under applicable law, your contractual terms, both, neither?

Can I get a list from you of everyone who has viewed, shared, or received my information through [org/product/service]?

- Do you provide individuals with an Accounting of Disclosures?
- If so, how/where can individuals request an Accounting of Disclosures? This is a great example of where it might make sense to direct individuals to where they can find more information (e.g., time to prepare, lookback period, etc.) versus including all of the details here.
- If your organization does not provide individuals with an Accounting of Disclosures, consider explaining why. You should also provide some general information on where individuals can look to obtain information on how their protected health information has been disclosed.

Do I need to opt in or provide my consent in order for some or all of my information to be shared through [org/product/service]?

- How your organization addresses this question will be highly dependent upon the type of organization it is and the laws to which it is subject.

Can I opt out of having some or all of my information shared through [org/product/service]?

- Does your organization provide individuals with the choice/ability to opt out of having their information accessed or disclosed through your org/service/product? If so, are there granular opt-out choices an individual can make, such as opting out of certain exchange purposes, or is opt-out only available on an all-or-nothing basis?
- If individuals have choices related to opting out and/or granular access management, it likely makes sense to provide a high-level explanation in your information handling practices and direct individuals to how/where they can find more information about your opt-out process, including how to submit a request and what individual should know about the effects of their opt-out choices and what they may wish to consider before deciding to opt out.
- If your organization does not provide individuals with the right/ability to opt out, why not? What options do individuals have if they do not want their information shared through your org/service/product?

Can I get a copy from you of all the information about me that is stored by your organization and/or that has been shared through [org/product/service]? Can I access health information about my minor child or an adult for whom I am the caregiver through [org/product/service]?

- Explain whether you provide individuals with access to their own information (or, as applicable, you may want to reiterate if you do not store any PHI and/or PII).
- As applicable, explain your policies on providing parents, guardians, legal agents, etc. with access to another individual's health information.
- If you do not provide this information directly to individuals, explain what rights and options individuals may have to obtain their information (e.g., HIPAA right of access).

Can I direct you to share my health information with a specific person or entity on my behalf?

- This could include allowing an individual to directly instruct your org/product/service to share information with a specified third party (e.g., an integration that allows the individual to connect their PHR), and/or this could be where you discuss whether/how your organization handles authorization-based disclosures.

How do you protect my information and keep it secure?

- This can be a hard one to condense, as we all know there is a lot that goes into keeping this information secure. One approach for breaking this down is to think about this in buckets of technical, physical, and administrative—even if you are not regulated under HIPAA—as this helps cover the bases without being overly technical or dense. For example:
  - Is the information encrypted in transit and at rest?
  - Where is the information stored and/or where are your servers located?
  - Do you use enforceable agreements and/or policies to ensure users comply with any access/use restrictions and that they keep their accounts secure?
  - Do you monitor access to / use of the information?

Is your organization regulated under HIPAA?

- While this may seem a bit "legalese," the answer/explanation should help unpack this. The key is for the individual to understand whether your organization is actually regulated as a Covered Entity or Business Associate and, therefore, subject to OCR oversight and enforcement.
- Specifically, the individual should understand whether they could avail themself of the OCR HIPAA Complaint Process versus, for example, whether your organization has merely agreed to comply with HIPAA privacy and security protections as a contractual standard (e.g., as a Non-HIPAA Entity (NHE) under the Trusted Exchange Framework and Common Agreement (TEFCA), including its Required Flow-Downs).
- This distinction is important for individuals to be aware of, as the individual is typically not a party to such HIPAA-like contractual requirements and, therefore, would have no rights under such contractual terms. Even if your organization contracts directly with individuals, offering them HIPAA-like data protections, there is a world of difference between being able to file an OCR complaint and needing to sue for breach of contract.

What happens if my information is inappropriately accessed, used, or disclosed? Will I be made aware? What will you do to make it right?

- There is a lot to unpack here that is going to depend upon whether/how your organization's handling of information is regulated, as well as what your contractual obligations may dictate. Two key recommendations are:
    - » Regardless whether your organization is subject to HIPAA, the FTC Health Breach Notification Rule, state breach notification requirements, contractual notification requirements, or any combination thereof, it is important to explain what constitutes an inappropriate access, use, or disclosure that would trigger notification to an individual.
    - » Avoid reflexive responses based on applicable law that fail to account for or explain your organization's role. For example: If your organization is a Business Associate, simply detailing what HIPAA says about Breach notification to affected individuals does not necessarily address the issue from the perspective of the individual. It is important to, first, explain that the Business Associate's obligation in these circumstances (however those are defined, as per the point above) is to notify the Covered Entity. Address who actually decides whether/when a Breach has occurred and notification to individuals is required.
- The issue of remediation and individual recourse for inappropriate access, use, or disclosure of health information relates closely to the discussion above regarding whether/how your organization is regulated and/or who has the right to enforce any contractual obligations your organization may have in such circumstances. However, it also provides an opportunity for those organizations that are not regulated under HIPAA to explain what other obligations they may have and to whom they are accountable.

How do I contact someone in your organization if I have additional questions or concerns about how my information is handled through [org/product/service]?

- Provide contact information for your Privacy Officer or other position/department responsible for responding to individuals' questions/concerns.
- At a minimum, contact methods should include both an e-mail address (or URL for a web-based contact form) and a toll-free phone number.

Additional Issues/Questions to Consider Addressing:

Sensitive Information: Are there any special protections for certain types of information about me?

Granular Information/Access Management:

Can I restrict or limit *who* is allowed to see or share my information and/or the reasons for which users are allowed to see or share my information through [org/product/service]?

Can I restrict certain types of information from being accessed and/or exchanged through [org/product/service]?

Amendments: What if I believe the health information being shared about me is incorrect? Will you honor my request to change my health information?

Deletion: Do I have the right to require your organization to delete all or some of my information?