5 Questions Patients Should Ask

About Health Care Information Security

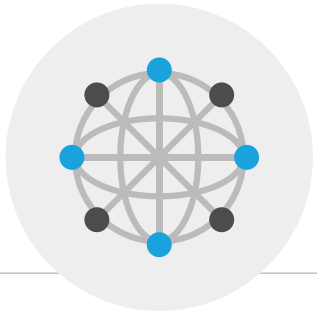
Patients need to understand the information security protections in place at their health care providers. Below, we've outlined a few questions that patients can ask of their providers to ensure that those organizations are applying appropriate and diligent stewardship of the data that they hold in trust.

Note that these are not the only possible questions that patients can ask their practitioners—only a starting point. These points are designed to initiate a conversation between the provider and the patient. Just like participatory medicine leads to better outcomes, a patient can initiate a dialog with their provider to stay informed about the security of their information and, in some cases, help improve the measures employed by that provider as a result. For more information about health care information security and governance of clinical information technology, go to **www.isaca.org/GEITforHealthcare**.

QUESTION 1

Who has access to my data?

A patient might reasonably think that only their physician and those directly supporting their care have access to their records. However, very often in practice, the audience is larger than that. Patients have the right under the Health Information Portability and Accountability Act (HIPAA) (45 CFR 164.524) to request the information about them maintained by the institution; looking through this information can inform a patient about who is accessing their information, what information is kept and (in some cases) circumstances under which that information is shared.



QUESTION 2

Do you have a security organization? What is the size of that organization?

In the US, HIPAA requires that organizations have a named privacy officer and security officer. So, it is almost certain that someone in the organization will be appointed as responsible for at least those two areas (since they need to for compliance with the law). However, the regulation does not require anything specific about the makeup of the organization supporting them: One health system might have a whole team supporting security, while another might have one person who's responsible for twenty things on their own.

ISACA®

QUESTION 3

What options are there to protect my privacy/anonymity?

Some institutions have mechanisms to allow them to provide care to patients who would otherwise garner too much unwanted attention—even in some cases from internal staff members. Some institutions will allow a patient to specifically request these protections should they ask. While not every institution can readily act upon a request like that—some can—so it makes sense to ask.

QUESTION 4

Is there a breach history?

Health and Human Services (HHS) currently maintains, as part of the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), a list of health care breaches impacting more than 500 individuals. This page is hosted via the Office for Civil Rights (OCR—the entity currently responsible for HIPAA enforcement). It provides a list that includes the name of the organization, the location, the type of organization, the date of the breach and a quick synopsis of what transpired. That page is located here: **https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.** Examine the list and ensure root causes have been addressed by your provider.

QUESTION 5

How will my test results, medical images or record be accessed by external physicians or affiliated clinics?

Sometimes, a larger institutional provider such as a hospital or health system will provide services on behalf of a physician or clinic that is not on staff with the institution. Of particular interest to patients might be the mechanisms used by their physician—and the hospital—for communicating those results to each other.

ISACA®