# The Dish: Security

# Protecting Participant Data

<https://www.youtube.com/watch?v=DswV-MueKMo>

## Scene

Eric Dishman speaking.

## Eric Dishman:

I was having a great conversation, not so long ago, with a lot of the frontline staff of the more than 125 clinics that are out there actively engaging with and enrolling participants in our protocol. And they said, “Our top question that we get from people—or certainly top three—is, ‘What’s going on with security? What are you doing to secure our data?’” I want you to know that this is one of our biggest concerns and our top priority: to make sure that we safeguard your data and maintain positive trust with you and the systems that we’re using to interact with you. If we lose that, then we would have the potential of losing the whole program.

So the first thing that we’re doing is making sure that we’re putting all of that data into a secure—what they call “the cloud”—you’ve probably seen commercials about this these days—stored in an environment like all the other banks and high-tech systems so that we’re getting the latest and greatest, you know, virus updates and security updates. This is not about putting some set of servers on the NIH campus in Bethesda. You want to use these commercial systems that are being constantly improved as the hackers get better at hacking into things.

We also go through a process called FISMA, F-I-S-M-A. I cannot remember what the acronym stands for. And if you want to get to sleep easily tonight, you can start reading about the FISMA process online. And this is a process that’s making sure that we’re using best practices in security and that we have our own security procedures and protocols in place and that we’re following those rules that we’ve actually set for ourselves. That includes also making sure that we’re holding all of our partners accountable to security at the same level that we are in all of their systems that may be sharing or sending any data around. This process involves constant testing. In fact, we just finished a hackathon with a company called HackerOne a couple of weeks ago that was a great method where they’re bringing good-person hackers who are experts at hacking but are not going to go do bad things with it to test and attack our systems as much as they can. And they get what’s called “a bounty,” right? They get paid based on finding these holes in our systems that we can then go fix. That’s a great method, to just let the hackers have at it and then go work to actually reduce any of those vulnerabilities that you have.

At the end of the day, what happens is my chief information security officer, who’s an expert in cybersecurity and who is reaching out to industry and government experts to making sure we’re doing everything that we can—we go through a process that they bring called authority to operate, or ATO. And ultimately, I, along with the chief information officer of NIH, sign off on that. And it also is not just a one-time thing. It’s saying, “These are the ongoing testing and things that you’re going to do to make sure you haven’t had a security breach.”

And God forbid we actually end up having one. There’s no such thing as a 100% guarantee. If a company or an organization is promising that your data can never be hacked, then they’re not being direct and transparent and completely honest with you. In spite of all these great measures, we say it could happen. And if it does, we have clear procedures for very quickly, very plain language, and very transparently telling you exactly what happened, how you might be affected, and what we would need to do going forward.

## Closing slide

*All of Us* Research Program

JoinAllofUs.org