Lets say that the U.S. government is holding a competition for what the best ideas on a new identity system are, and the winner becomes the implementation they used. A system that would make it impractical for identities to be stolen. Convince me this solution is right or wrong. Here are the details of a submission:

Usb-like device: Every person receives a sort of mini usb like device with minimal computation capabilities that contains all their personal information like age, medical history, etc. all encrypted by a unique public key. The private key is stored on this device in an unreadable, immutable area which can only be used to decrypt internal data. The government's public key is stored internally and immutably so that way it can validate any api that attempts to access data that is government approved. The data has to be sectioned in a structured way to allow for effective api access.

Government Web App: This application would be able to connect to a cloud system run by the government for the sole purpose of allowing traffic of personal information, and it would contain a way to further verify one's identity. For example at the time of receiving one's identity, they would encode some biometrics that can be verified with a camera(face, retinal), storing only the uninterpretable descriptors created by a recognition model. In this way, simply stealing the usb like device is not enough to verify identity. These biometrics would be stored in the government's cloud database, but because they are encoded descriptors, having this data exfiltrated would not change much about the overall security of the scheme. Each time a person is verified, the most recent few significantly different verified descriptors are kept while the old ones are thrown out so any changes in face are accounted for. Additionally, more in depth biometrics that require specific equipment like real-depth facial recognition, or finger prints.

Government No-Network App: the government releases an application for managing communication of personal identification. It contains their public key hard-coded in. It connects only to the Government web app and allows you to access PII on the usb-like device. It never sees the private key, but does have access to data that is sent over. It has limited access to the data and has a structured API so only specified data can be sent(like medical history), and others can simply be checked(like age>18).

Verifying Identity: The mini usb like device is plugged into a computer, and the government No-Network application is run. First the usb-like device checks if the application is actually the government's. Then the government application checks if the usb contains the private key to the given public key. Once that is passed, a picture is taken and the biometrics are checked and compared to the government's database of descriptors for the associated public key through the Government Web App. This process fully confirms identity and can now be used instead of SSN, Name, birth date, etc. for all things. Rather than storing someone's PII, they only store the public key of the person.

You send information: Step 1) Your identity is verified through the two government apps. Step 2) A verified person requests certain information from you through their No-network app. That request is sent to the web app and then given to your no-network app along with their public key

and additional information(maybe: selfie with verified face and full name). Step 3) You approve the parts of the request you want and specify an amount of time the person can view the data for(Max 1 Day from opening, max 1 week after send date). The specified data is taken from the usb like device. Step 4) Your no-network application encrypts the data using the other person's public key, and sends it to them through the web app along with the specified amount of time it can be viewed. Step 5) The other person's no-network application receives your encrypted data through the web app, displays it, and completely destroys all traces of it once the allowed time runs out or the person says they no longer need it.

Updating information: A person sends you an update request to your information from their no-network app, indicating a particular section the data should be added to. No-network app adds it to your usb-like device, and immediately wipes any traces of the data on the app.

Losing your usb-like device: Go to a government site and verify your identity using the in-depth biometrics. They will give you a new usb-like device and switch your old public key out with your new public key in their key-biometric database. There would also be a separate database of key changes so that one's history can be tracked. If someone attempts to use the old public key, they would not be found in the database of key-biometric pairs and would be denied authentication by the government web app. If one wants a full history of activities by one person, they would pull