The recommendation:

Initiate discussions with relevant stakeholders to determine what constitutes reasonable and appropriate security measures commensurate with the offering of services that involve the gathering of sensitive health and financial information. Such a discussion could include identifying what falls within the categories of "sensitive health and financial information" and what metrics could be used to measure compliance with this safeguard.

This recommendation has it's genesis in the GAC Beijing communiqué https://www.icann.org/en/news/correspondence/gac-to-board-11apr13-en.pdf specifically page 8 point 3:

Registry operators will require that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law and recognized industry standards.

This resulted in the designation of GAC category 1 strings – see https://newgtlds.icann.org/en/applicants/gac-advice/cat1-safeguards . The application framework, amongst others specifies:

3. Registry operators will include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision requiring that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law.

Note the dropping of 'recognized industry standards'.

The actual text that made it into the agreements, taken from the .Pharmacy agreement – https://www.icann.org/resources/agreement/pharmacy-2014-06-19-en Specification 11, #3 g:

> *g. Registry Operators will include a provision in their Registry-Registrar Agreements that requires registrars to include in their Registration Agreements a provision requiring that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law.*

Not, being a lawyer, I did scan the document for what would be 'applicable law' - and whilst it is not 100% clear, it is my interpretation that the applicable law would be at least, but not necessarily exclusively: a) the law where the registrant is incorporated; and b) the where the registrant conducts business.

It is important to note that the mandated security measures, in all cases are tied back to 'applicable law'. As such, what constitutes 'reasonable and appropriate security' is **already defined, namely it is 'defined by applicable law'**. No process initiated by our recommendation will trump 'applicable law'.
It is further my opinion, that this recommendation sets up an impossible task. For example, the potential 'applicable law' includes every registrant jurisdiction, and the enquiries into determining what services the registrants in these strings is potentially open ended.

The recommendations put forth in recommendation 23, to be more granular in data collection will address the main nexus of our rationale, which was to see if there has been impact of the safeguards.