Florida Elder Law Risk Detector Data Storage FAQs – March 2020

For more questions or more information, please contact:
Sarah Halsell, halsellsk@elderaffairs.org

- **What software powers the Risk Detector?**

The Risk Detector uses web-based software called Neota Logic System (NLS). NLS is provided as a platform-as-a-service (PaaS) and is hosted by Amazon Web Services (AWS), a secure, enterprise-level cloud services platform. NLS is designed and configured at AWS for security, fault tolerance, high availability, and easy scaling to assure good performance at high levels of use. Most Neota Logic clients are large law firms and financial institutions with high security requirements that Neota Logic meets. Neota Logic and Pro Bono Net have a partnership to leverage the NLS software in support of access to justice initiatives, including the Risk Detector program.

- **What data is stored, and where?**

Currently, the Legal Risk Detector saves a small amount of data from each session via the Neota Data Storage (NDS) feature. For the Florida Risk Detector pilot, this will include the organization conducting the screening, the date of session, the type of session (Express or Standard), name of community partner user and client, client age, county, the relevant risk, and the final report generated by the app, which is stored as mime file and can be downloaded as PDF document. This saved saved data is encrypted during transmission between a client/browser and NLS (HTTPS/TLS) and also "at rest" (encrypted while it sits in NDS).

- **Who has access to the stored data?**

Neota Logic and Pro Bono Net system administrators have access to the NDS-stored data for the limited purposes of support and maintenance through a password-protected log-in. The purpose of this access is similarly limited to technical/project support and reporting on anonymous, aggregated data.

- **What about ethical obligations of the Community Partners using the Risk Detector with regard to client confidentiality?**

The Risk Detector is very similar to any other referral mechanism used by Community Partners, or other government or non-profit organizations that wish to refer a client to free, civil legal services. Community Partners can choose how much client information they want to divulge (e.g. Community Partners are able to leave some client information out of the Legal Risk Detector screening if they are concerned with sharing any of the information requested). However, keep in mind the following: 1) the legal services organization that receives the referrals will need enough information to follow up with the individual client, and therefore you must be clear in your training if the legal services organization requires certain information to be provided; and 2) as long as the Community Partner is properly trained, the Community Partner will be making the client aware that one of the main purposes of the Legal Risk Detector is to connect the client to free, civil legal services, and that in order to do so, the Community Partner must provide some basic client information and problem description to the legal services organization (i.e. the Community Partner should be obtaining the client's consent).