# RadResponder Network

A secure, flexible architecture designed to meet the needs of modern emergency response

Who has access to the RadResponder Network?

RadResponder is a product of collaboration among FEMA, DOE/NNSA, and EPA, and is provided free to federal, state, local, tribal, and territorial organizations and industry partners that have roles or responsibilities in radiological/nuclear emergency response. Prior to joining the Network, new users are vetted first by the organizations that employ them, and second by the RadResponder Admin Team before receiving an account. Organizations that are new to the RadResponder Network must be sponsored by an existing organization that can confirm their role in the radiological/nuclear community.

Who can see my data?

Partnership capabilities provide organizations with the flexibility to manage with whom and under what circumstances radiological data is shared. Access to event data can be customized on an event-by-event basis, and access for an individual or organization can be revoked at any time, even after an event has closed.
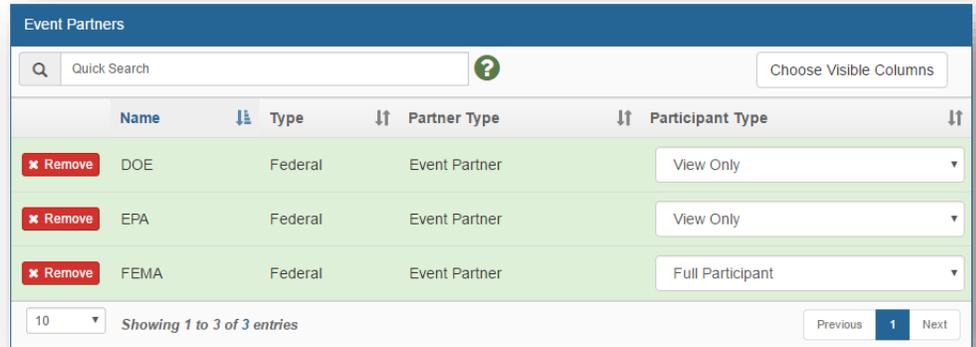
Organizations always maintain the right *not* to share their data, and can make events accessible to only their organization or select personnel. While all organizations have full control over their own event space, some are subject to additional restrictions while interacting within the Network at large. For example, corporate organizations, such as equipment manufacturers seeking to integrate with RadResponder, do not have access to the list of organizations or personnel that are members of RadResponder.

How is my data stored and protected?

Radiological data initially recorded in the mobile application is uploaded automatically to the RadResponder server via a secure protocol. In a cellular-denied environment, data is cached locally and uploaded automatically once a connection is detected.

The RadResponder server is hosted in the FedRAMP-approved Microsoft Azure Cloud environment. This geo-redundant infrastructure automatically scales in response to increased usage, and provides automatic fail-over capabilities for the website in the case that an entire Microsoft data center is lost due to a major catastrophe. In addition, the RadResponder mobile applications are the first mobile applications to undergo DHS's new security vetting process, and the RadResponder Team runs several routine vulnerability scans to check for potential security issues in the RadResponder website.

Personally Identifiable Information (PII)

RadResponder collects only limited, non-sensitive PII (name, organization, work email, work phone number) to be associated with the radiological data that an individual records, for the purposes of maintaining data quality.

For more information, please contact the RadResponder Team at support@radresponder.net

FEMA | CBRNE OFFICE | 500 C Street SW Washington, D.C. 20472
1-202-646-8269 | http://www.radresponder.net | support@radesponder.net