

AUGUST 28, 2025 | PUBLICATION

Client Alert: Florida's New Proposed "Data Breach Transparency Rule"

The Agency for Health Care Administration (AHCA) has proposed a new Florida Administrative Code Regulation (Rule) regarding "data breach transparency." The Rule will apply to the following:

- Laboratories authorized to perform testing under the Drug-Free Workplace Act;
- Birth centers;
- Abortion clinics;
- Crisis stabilization units;
- Short-term residential treatment facilities;
- Residential treatment facilities;
- Residential treatment centers for children and adolescents;
- Hospitals;
- Ambulatory surgical centers;
- Nursing homes;
- Assisted living facilities;
- Home health agencies;
- Nurse registries;
- Companion services or homemaker services providers;
- Adult day care centers;
- Hospices;
- Adult family-care homes;
- Homes for special services;
- Transitional living facilities;
- Prescribed pediatric extended care centers;
- Home medical equipment providers;
- Intermediate care facilities for persons with developmental disabilities;
- Health care services pools;
- Health care clinics; and
- Organ, tissue, and eye procurement organizations.

These businesses are termed "Providers" under the Rule. This proposed Rule will require that Providers: (i)

INDUSTRY SECTOR

Health Care

SERVICE LINE

Technology, Data Privacy,
Cybersecurity & AI

RELATED PROFESSIONALS

Grant P. Dearborn
Virginia "Ginny" Dailey

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

report an information technology incident to AHCA no later than 24 hours after the Provider “reasonably believes an information technology incident may have occurred;” (ii) Providers must have a “continuity plan.”

“Information technology incident” means “an observable occurrence or data disruption or loss in an information technology system or network that permits or is caused by unauthorized access of data in electronic form.” Good faith access by an authorized employee does not constitute an information technology incident, provided that the data is not used in an unauthorized manner or for an unauthorized purpose.

Furthermore, “data” means “information and representations of information, knowledge, facts, concepts, documents, instructions, images and recordings whether humanly-perceivable or machine-readable, in any form, and whether in use, storage, physical or electronic transit, or presented on a display device.” This will require a separate analysis beyond any analysis under the Health Insurance Portability and Accountability Act (HIPAA).

The “continuity plan” must include the following elements: (i) a written policy detailing procedures and information designed to maintain critical operations and essential patient care services during an interruption of normal operations; (ii) a procedure for the regular performance of secure, redundant on-site and off-site data backups and verification of the restorability of backed-up data; and (iii) requirement that off-site backups must not be stored outside the continental United States.

Additionally, a Provider must present to AHCA, if requested:

- (i) A police report, incident report, or computer forensics report;
- (ii) A copy of the policies in place regarding information technology incidents;
- (iii) Information disclosed;
- (iv) Steps that have been taken to rectify the incident; and
- (v) The continuity plan.

These are in addition to the requirements in HIPAA. It is advisable for health care providers to review this proposed rule and provide comments to AHCA.

If you have questions or need more information, please contact Grant Dearborn or Ginny Dailey.