HIGHER EDUCATION FIELD BRIEF

For every college that takes federal student aid

INCIDENT RESPONSE

Who do you have to notify, and how fast?

INSIDE THIS BRIEF

01-05 Five reporting requirements

NEXT The proposed federal rule

ACTION Who owes what, and what to have ready

Dan Didier

Co-founder & Principal, CyberRisk One

THE SHORT VERSION

One incident can trigger several reporting requirements.

- **They come from different places**, including your student aid agreement with the Department of Education, federal rules, research contracts and state laws.
- **They have different triggers.** Some start on a suspected breach, others on discovering an incident or a materiality decision. The proposed CIRCIA rule would add a ransom payment.
- **They don't all apply to every school.** Public, nonprofit and for-profit schools differ, and so do schools with a hospital or defense research.

THE ONE EVERY AID SCHOOL SHARES

> If your school takes federal student aid (Title Iv), a suspected breach of aid applicant or other sensitive information must be reported to Federal Student Aid **immediately.**

Federal Student Aid Dear Colleague Letter GEN-15-18

REQUIREMENT 1 / FEDERAL STUDENT AID

Report it immediately.

Applies to every school that takes federal student aid (Title IV).

- **Where it comes from.** The Student Aid Internet Gateway agreement your school signed. It's a contract term, so you won't find it by searching the regulations.
- **What triggers it.** An unauthorized disclosure, or an actual or suspected breach, of aid applicant information or other sensitive information.
- **The deadline.** The agreement requires immediate reporting. Prepare to report while the investigation is still underway.
- **How.** The breach intake form or reporting mailbox. Check the current instructions on fsapartners.ed.gov.

> Report a suspected breach through FSA's current reporting channel **while the investigation continues.**

REQUIREMENT 2 / GLBA

Who enforces GLBA at your school?

Applies to every federal aid school through the GLBA Safeguards Rule. Who enforces it depends on the school.

- **Every aid school.** The Department of Education enforces it through the student aid compliance audit, and repeated findings can affect Title IV participation.
- **Schools under FTC jurisdiction, mostly for-profit.** Notify the FTC as soon as possible, and within 30 days after discovering a notification event involving unencrypted customer information of at least 500 consumers. Unauthorized access is presumed to be acquisition unless reliable evidence shows otherwise, and encrypted data counts as unencrypted if an unauthorized person accessed the key.
- **The 30 days start** on the first day the event is known, or would be known with reasonable diligence, to any employee, officer or other agent other than the person who committed it.

> Have counsel confirm **whether your school is under FTC jurisdiction.**

REQUIREMENT 3 / HEALTH RECORDS

HIPAA or FERPA?

Applies to schools that may have HIPAA covered operations, such as an academic medical center, a hospital, or a clinic that bills insurance electronically.

- **Under HIPAA.** After a breach of unsecured protected health information, notify affected people without unreasonable delay and within 60 days of discovery. If 500 or more people are affected, notify HHS in the same window, and prominent media when more than 500 residents of one state or jurisdiction are affected. Report smaller breaches to HHS within 60 days after the end of the calendar year they were discovered.
- **Many student health records aren't HIPAA records.** At a FERPA school, what a campus clinic keeps on its own students is often an education or treatment record under FERPA, and HIPAA leaves those records out of protected health information.
- **FERPA has no breach notice deadline of its own.** State laws can still apply.

> **Have counsel and the clinic decide** which operations and records fall under HIPAA and which under FERPA, before an incident.

REQUIREMENT 4 / RESEARCH AND CONTRACTS

Read the contract.

Applies to schools doing defense research or holding other federal contracts and awards.

- **Defense contracts with DFARS 252.204-7012.** Report covered cyber incidents to the Department of Defense within 72 hours of discovery. Keep images of affected systems and monitoring data for at least 90 days after you report.
- **Other federal awards can carry their own incident clauses.** The obligation lives in the contract or award terms.
- **Research systems and data can sit outside IT's view.** Labs, the grants office and principal investigators need to know these reporting requirements exist.

> Ask the grants office for **a list of active contracts with reporting clauses.**

REQUIREMENT 5 / STATE LAWS

Check the laws where affected people live.

Applies to every school.

- **Every state has a breach notification law.** Each one protects certain personal information about its residents, who can include your students, staff, alumni and applicants.
- **Generally, each state's law covers its own residents, so where the affected people reside decides which laws apply.** One campus incident can trigger requirements in several states.
- **Deadlines and recipients vary.** Some states set a fixed number of days, and many also require notice to the attorney general.

> **Keep a current list** of the states where your students, staff, alumni and applicants live, and the rules that go with them.

COMING NEXT / CIRCIA

A federal requirement that isn't here yet.

As proposed, applies to every school that takes federal student aid, plus K-12 districts with 1,000 or more students.

- **What the proposal says.** A covered entity would report a covered cyber incident to CISA within 72 hours after it reasonably believes the incident occurred, and a ransom payment within 24 hours after making it.
- **Where it stands.** The final rule went to the White House budget office (OIRA) for review on October 1, 2026, per the OIRA review listing. As of early November 2026, it had not been published in the Federal Register.
- **Nothing under CIRCIA is required yet.** The final rule will establish which colleges are covered and when reporting becomes mandatory.

> Test **each reporting requirement** in a tabletop, including its trigger, required information and submission process.

WHO OWES WHAT

Find your school on the list.

IF YOUR SCHOOL	WHAT YOU MAY HAVE TO FILE	DEADLINE
Takes federal student aid	Report to Federal Student Aid	**Immediately**
Every school	State breach notices, if triggered	**Varies**
Is under FTC jurisdiction, usually for-profit	FTC notice of a notification event, 500 or more consumers	**30 days from discovery**
Has HIPAA covered operations	Required HIPAA breach notices	**60 days***
Has contracts with DFARS 252.204-7012	Report covered cyber incidents to the Department of Defense	**72 hours from discovery**
Is part of an SEC reporting company	Registrant assesses whether an Item 1.05 Form 8-K is required	**4 business days****
Is covered by the final CIRCIA rule	Report to CISA	**72 / 24 hours, as proposed**

A public or nonprofit school usually owes the first two rows, plus whichever of the rest fit. Confirm your list with counsel. *People without unreasonable delay, within 60 days; HHS timing depends on breach size. **Generally, after the incident is found material, a decision the registrant must make without unreasonable delay after discovery.

WHAT TO HAVE READY

Four things to have ready before an incident.

01 **A plan that's ready to use**

Approved by leadership and available to the people who will carry it out.

02 **Your reporting requirements, written down**

Each one with its trigger, deadline and recipient.

03 **Notice templates, reviewed in advance**

A draft for each recipient, reviewed by counsel.

04 **A named owner for each report, with a backup**

Authorized to report a suspected breach early.

> Then practice it in a tabletop. **CyberRisk One** runs incident response tabletops for colleges.

This is our summary as of November 2026 and is not legal advice. Sources: FSA GEN-15-18, GEN-16-12, GENERAL-23-09; 16 CFR 314; 45 CFR 164; DFARS 252.204-7012; SEC Form 8-K Item 1.05; 89 FR 23644; OIRA review listing, RIN 1670-AA04.