RadarFirst

CYBERSECURITY NOTIFICATION OBLIGATIONS

Healthcare | U.S. Federal

Disclaimer

The information provided in this presentation does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this presentation are for general informational purposes only. Information in this presentation may not constitute the most up-to-date legal or other information. This presentation contains links to third-party websites. Such links are only for the convenience of the reader; RadarFirst does not recommend or endorse the contents of the third-party sites.

INTRODUCTION

When cyber incidents occur, organizations have a responsibility to report them to various agencies, partners, and stakeholders.

In a recent report, the Department of Homeland Security found that there are **52 cyber incident reporting requirements, either in effect or proposed, across the Federal Government and 22 agencies**.

Current requirements are derived from a patchwork of regulations and authorities, many with unique and sometimes overlapping information requirements, timelines, and submission methods.

To simplify U.S. Federal reporting for Healthcare organizations, RadarFirst has collected the following effective and proposed reporting requirements for cybersecurity notification obligations, their timelines, triggers, and reporting thresholds.

RadarFirst

REGULATIONS

HHS

- 45 C.F.R. §§ 164.400-414 **

FTC

- Health Breach Notification Rule 16 C.F.R Part 318 ****

FDA

- 21 C.F.R Part 803 ****
- 21 C.F.R Part 806 *

**** Obligation includes urgent notification, i.e. "promptly" or "as soon as possible."***

**** Obligations includes time-based notification.***

***** / **/ ** Regulation includes multiple obligations unique timelines and/or unique recipients.***

Department of Health and Human Services (HHS)

Requirement

The HIPAA Breach Notification Rule (In Effect) 45 C.F.R. §§ 164.400-414

Entities Subject to Reporting Requirements → Timeline and Triggers

"HIPAA covered entities and their business associates"

→ Must notify if **over > 500 or more individuals** affected must notify the HHS **without unreasonable delay** and **no later than 60 calendar days** from the discovery of the breach.

"HIPAA covered entities and their business associates"

→ Must notify if **less** than **< 500 or more individuals** or affected must notify the HHS **within 60 calendar days** from the discovery of the breach.

Reportable Cyber Incidents / Threshold

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that **compromises the security or privacy** of the protected health information. **An impermissible use or disclosure of protected health information is presumed to be a breach.**

- Breaches affecting **500 or more individuals**
- Breaches affecting **fewer than 500 individuals**

"An impermissible use or disclosure of protected health information is **presumed to be a breach unless the covered entity or business associate,** as applicable, **demonstrates** that there is a **low probability** that the protected health information has been compromised **based on a risk assessment.**

Federal Trade Commission (FTC)

RadarFirst

Requirement

Health Breach Notification Rule (In Effect)

Entities Subject to Reporting Requirements → Timeline and Triggers

Personal Health Records (PHRs) vendors, related entities, and third-party service providers **must report** to the:

→ **Affected Individuals: "Without unreasonable delay"** and **no later than 60 calendar days** from the discovery of the breach.

→ **FTC and over > 500 or more individuals** affected: **As soon as possible** and in **no later** than **ten business days** following the date of discovery of the breach.

→ **FTC and less than 500 individuals** affected: "**No later** than **60 calendar days** following the **end of the calendar year**, **documenting breaches** from the **preceding calendar year**."

Personal Health Records (PHRs) vendors and related entities **must notify**:

→ **Prominent state** or **jurisdiction media** outlets **and over 500 or more individuals** affected in **that State** or **jurisdiction: following discovery** of breach or security.

Reportable Cyber Incidents / Threshold

"Breach of security": "Unsecured PHR identifiable health information of an **individual** in a personal health record, **acquisition** of such information **without the authorization of the individual."**

Unauthorized acquisition: "Includes **unauthorized access to unsecured PHR identifiable health information** unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information."

Food and Drug Administration (FDA)

Requirement

Medical Device Reporting (In Effect)
21 C.F.R Part 803

Entities Subject to Reporting Requirements → Timeline and Triggers

"Device User Facilities" or "Importers"

→ Must notify the manufacturer and FDA **no later 10 workdays** after the day the user facility becomes **aware of a death or serious injury to a patient** in the facility.

→ Must report to the manufacturer **not later than 10 workdays** after the day that the user facility becomes aware of information that reasonably suggests that a device has or may have caused or contributed to a serious injury. If the manufacturer is not known, the user facility must submit this report to FDA.

"Medical Device Manufacturer"

→ Must submit a "**5-day report"** within 5 work days after the manufacture is aware of an event

- Where **remediation** is **required** "to **prevent unreasonable or substantial harm** to the **public health**"
- Where the **FDA has made a written request** for the submission of 5-day reports (21 C F R 803.10(c), 803.20, 803.53).

→ Must submit **no later than 30 calendar days** after the day the manufacturer is **aware of reportable death, serious injury, or malfunction.**

Reportable Cyber Incidents / Threshold

"A **reportable death, serious injury, or malfunction** is based on **information a manufacturer receives** or otherwise becomes aware of, **from any source**, which reasonably suggests that one of its marketed devices has done" **either one** of the following:

- **May have caused or contributed to a death or serious injury**
- **Malfunctioned** and the **device or a similar device marketed by the manufacturer** would be likely to **cause or contribute to a death or serious injury** if the malfunction were to recur.

Food and Drug Administration (FDA)

RadarFirst

Requirement

Corrections and Removals of Medical Devices (In Effect)
21 C.F.R 806, Medical Devices

Entities Subject to Reporting Requirements → Timeline and Triggers

"Manufacturers" and **"Importers"**

→ **Within 10 working days** of the time the manufacturer or importer **initiates the correction or removal.**

Reportable Cyber Incidents / Threshold

"Each device manufacturer or importer must **submit a written report to FDA of any correction or removal of a device(s) if it was initiated** by such manufacturer or importer t**o reduce a risk to health posed by the device** or to r**emedy a violation of the Federal Food, Drug, and Cosmetic Act** caused by the device, which may present a risk to health. If this criterion is met, a report must be made e**ven if the event was caused by user error. "**

"A report **is not required** if the information has already been **provided to FDA** under **Medical Device Reporting** (21 C F R 803) or **Repurchase, Repairs or Replacement of Electronic Products** (21 C F R 1004) or if the **action was initiated by an FDA** order under FDA's device recall authority (see section 518(e) of the Federal Food, Drug, and Cosmetic Act and 21 C F R 810). "

RadarFirst

Enterprise Value is at Risk

Existing tools and manual processes cannot scale with today's complexity.

Challenges

- Increased incident volumes
- Changing laws and regulations
- Assessment / decision consistency
- Short notification timelines
- Stretched resource capacity

Impact

- Missed notification deadlines
- Regulatory audits and fines
- Customer loss
- Significant external legal costs
- Staff retention / attrition

Outcomes

- Decreased enterprise value
- Brand / reputational damage
- Lost customer / partner loyalty
- Inability to scale
- High departmental overhead

Operationalize Notification Obligations with Radar® Compliance

Radar® Compliance is a rules and assessment engine that can be configured to satisfy internal and external compliance notification requirements and obligations, such as:

- Cybersecurity events
- Third-party contractual mgmt
- Auditable reporting
- And more

Talk to a RadarFirst specialist to learn how you can define your own notification triggers and obligations with **Radar® Compliance**.

Capital One · VOYA FINANCIAL · BNY MELLON · CNO FINANCIAL GROUP · Texas Capital Bank · RAYMOND JAMES · Hyundai Capital

Thank You!