



**The Rogosin Institute**  
**Sites: All Centers**  
**Policies and Procedures Manual**  
**Number: RI L135**  
**Page 2 of 7**

---

family member or neighbor;

- A Workforce Member providing patient information to the wrong patient or outside agency; or
- A Workforce Member improperly disposing of patient information.

Rogosin shall not require individuals to waive their rights to file a complaint with the Secretary of the Department of Health and Human Services (herein known as "Secretary of HHS"), as a condition of the provision of treatment, payment, enrollment in health plan, or eligibility for benefits.

**Investigation:**

All reported matters will be reviewed by the Office of Corporate Compliance and Privacy. As appropriate, and in collaboration with other Rogosin departments, as needed, an investigation and risk assessment will be conducted to determine among other things, the level of compromise to the PHI and if the events of the incident meet the legal standard of a reportable privacy breach<sup>3</sup>. If determined that a breach of patient privacy has occurred, the Privacy Office shall comply with all applicable federal and state breach notification and reporting requirements.

The Privacy Office will maintain all pertinent documentation, including breach logs, evidence that all required parties were notified in the event of a breach, rationale if an incident was determined to not meet the definition of breach, and documentation of notification delay requests.

**Breach Determination - Risk Assessment and Breach Exceptions:**

An impermissible use or disclosure of PHI is presumed to be a breach unless the investigation determines that there is a low probability that the PHI has been compromised, based on a risk assessment which considers the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

In addition, the circumstances contributing to the presumed breach should be reviewed to determine if any meet the following breach exceptions:

1. An unintentional acquisition, access, or use of PHI by a Workforce Member or person acting under the authority of Rogosin or business associate, if such acquisition, access, or use was made in good faith, within the scope of

---

<sup>3</sup> **Breach** - the acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

**The Rogosin Institute**  
**Sites: All Centers**  
**Policies and Procedures Manual**  
**Number: RI L135**  
**Page 3 of 7**

---

authority, and was not further disclosed in a manner impermissible by the HIPAA Privacy Rule.

2. An inadvertent disclosure of PHI by a person authorized to access PHI at Rogosin or business associate of another person at the covered entity<sup>4</sup> or a member of the organized health care arrangement (OHCA)<sup>5</sup> in which the covered entity participates, and was not further disclosed in a manner impermissible by the HIPAA Privacy Rule.
3. Rogosin or a business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

**Breach Notification Requirements:**

Breach notification shall be provided only when the breach involved unsecured PHI.<sup>6</sup> For these cases, notification will be provided to (i) the affected individual(s); (ii) the Secretary of HHS ; and (iii) the New York State Attorney General's Office. In the event the breach affects five hundred (500) or more individuals, Rogosin will also notify the media. Follow this [link](#) for notification framework.

**Breach Notices:**

Upon determination of a breach, the Privacy Office shall take the following steps, without unreasonable delay and no later than 60 days following the discovery<sup>7</sup> of the breach, except as indicated below:

For a single breach involving 500 or more individuals:

1. The affected individuals will be notified in writing of the breach by the Privacy Office in collaboration with the Patient Services Department;
2. The Privacy Office will submit an electronic breach report to the Secretary of HHS via their website; and
3. The Office of Public Affairs in consultation with the Privacy Office will place a notice, in the form of a press release, in prominent media outlets serving the state or jurisdiction where the affected individuals reside.

---

<sup>4</sup> "Covered entity" refers to (1) health plans; (2) health care clearing houses; and (3) health care providers who electronically transmit health information.

<sup>5</sup> An organized health care arrangement ("**OHCA**") - A clinically integrated health care setting in which individuals typically receive health care from more than one health care provider, or an organized system of health care in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement and/or participate in joint activities involving utilization review, quality assessment and improvement activities or payment activities.

<sup>6</sup> Unsecured **PHI** - Protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of Health and Human Services.

<sup>7</sup> **Discovery** - Breach is treated as having been discovered as of the first day on which the breach is known or should have been known by the covered entity or business associate, exercising reasonable diligence.

**The Rogosin Institute**  
**Sites: All Centers**  
**Policies and Procedures Manual**  
**Number: RI L135**  
**Page 4 of 7**

---

For a Breach involving fewer than 500 individuals:

1. The affected individual(s) will be notified of the breach by the Privacy Officer, in conjunction with the Patient Services Department; and
2. The Privacy Office will maintain an electronic log detailing any such breach and submit an annual report electronically via the Secretary of HHS website, no later than 60 days after the end of the calendar year in which the breach(s) occurred.

**Breach Notification to Affected Individual(s):**

Breach notification shall be provided to affected individuals when the risk assessment determine there is more than a low probability that PHI has been compromised and where no exceptions were met.

**Written Notice:**

Notification will be sent via first-class mail to the last known address of the individual or, if the individual agrees, by electronic mail. If an affected individual is known to be deceased, written notification via first-class mail shall be sent to the address of the next of kin or personal representative of the individual.

Written notification to affected individuals shall include, at a minimum:

- a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- b. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
- c. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
- d. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- e. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, or postal address.

Substitute Notice: When there is insufficient or out-of-date contact information for the affected individual(s) substitute notification will be provided. For cases involving 10 or more affected individuals, substitution notice will be conspicuously posted for a minimum of 90 days (i) on Rogosin website or (ii) placed in major print or broadcast media in geographic areas where the affected individuals likely reside.

A toll-free number will also be made available so that individuals can learn whether

**The Rogosin Institute**  
**Sites: All Centers**  
**Policies and Procedures Manual**  
**Number: RI L135**  
**Page 5 of 7**

---

their unsecured protected health information may be included in the breach.

For cases with fewer than 10 individuals, substitute notification may be provided by an alternative form of written notice, telephone, or other means.

In addition to written or electronic notification, affected individuals may also be contacted via telephone or other means when the Rogosin deems there is an urgent need to do so.

**Breaches of PHI discovered by Business Associates:**

Pursuant to HITECH requirements, business associates must communicate any breach of PHI to Rogosin. Following receipt of such communication, Rogosin 's Privacy Officer will prepare notification to affected individual(s) and others as necessary in accordance with this policy.

**Law Enforcement Delays:**

When a law enforcement official informs the Rogosin that notification, notice, or posting required under this policy would impede a criminal investigation or cause damage to national security, the Privacy Office shall delay notification:

1. if law enforcement provides a written statement requesting delay and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
2. if the statement is made orally by law enforcement, the Workforce Member should document the statement, including the identity of the official making the statement. If the request is deemed reasonable by the Privacy Office, then the Privacy Officer will delay the notification, notice, or posting temporarily for no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time specifying a different time period.

**New York State Breach Notification Requirements:**

The Privacy Office shall also comply with New York State (NYS) Laws related to breach notification requirements and will notify, the NYS Attorney General; and the Department of State's Division of Consumer Protection, when applicable.

**Access of PHI by Rogosin Workforce:**

If an Rogosin Workforce Member inappropriately accesses or discloses a patient's PHI for anything other than a legitimate work-related purpose, the Workforce Member will be subject to corrective action as set forth in Rogosin 's Policy C140: "Corrective Action to Deter Violations of Patient Privacy and Security." For non-Rogosin employed Workforce Members who violate Rogosin Privacy or Information Security policies, the Privacy Office, in coordination with Human Resources and other departments, as appropriate, will work with the person's respective employer

to enforce applicable corrective action.

**DEFINITIONS:**

**Breach** is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

**Business Associate** is a person or entity, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of protected health information or personal identifiable information. Business Associate functions or activities on behalf of a covered entity include but are not limited to claims processing, data analysis, utilization review, and billing.

**Organized Health Care Arrangement (OHCA)** A clinically integrated health care setting in which individuals typically receive health care from more than one health care provider, or an organized system of health care in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement and/or participate in joint activities involving utilization review, quality assessment and improvement activities or payment activities.

**Protected Health Information ("PHI")** all individually identifiable health information held or transmitted by health care providers, including Rogosin and its employees, or their business associates,, in any format, that is created or received by Rogosin and relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient or the past, present, or future payment for the provision of health care to a patient; or information about the patient which can reasonably be used by a third-party to identify the patient (i.e., names, address, social security number, etc.).

**Staff** means employees, medical staff, residents, fellows, volunteers, trainees and other persons whose conduct in the performance of work for Rogosin is under the control of Rogosin whether or not they are paid by Rogosin.

**REFERENCES:**

Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. 164.514(f)

**RESPONSIBILITY:**

**The Rogosin Institute**  
**Sites: All Centers**  
**Policies and Procedures Manual**  
**Number: RI L135**  
**Page 7 of 7**

---

Privacy Officer, Security Officer  
VP Audit and Compliance, Associate General Counsel

**POLICY DATES:**

**ISSUED:** December 2011

Revised: September 2013; July 2016; December 2021; April 2023

**Reviewed:** November 2015; September 2017; September 2019; December 2021; April 2024, **February 2025**