

# OREGON STATE HOSPITAL

## POLICY ATTACHMENT

---

<b>Procedures A:</b>	Incident Response and Reporting an Incident	<b>POLICY: 1.003</b>
----------------------	---	----------------------

---

<b>POINT PERSON:</b>	Director of Quality Management
----------------------	--------------------------------

---

<b>APPROVED:</b>	Interim Superintendent	<b>DATE: NOVEMBER 3, 2025</b>
------------------	------------------------	-------------------------------

---

<b>SELECT ONE:</b>	<input type="checkbox"/> New policy attachment	<input type="checkbox"/> Minor/technical revision of existing policy attachment
	<input type="checkbox"/> Reaffirmation of existing policy attachment	<input checked="" type="checkbox"/> Major revision of existing policy attachment

---

### I. INCIDENT RESPONSE

- A. Staff who are involved in a reportable event shall prioritize staff and patient safety in the immediate response.
- B. If able, staff must take any reasonable actions or remediations to prevent the incident from reoccurring.
- C. Staff should consider the preservation of evidence and consult with security for proper preservation and collection.
- D. OSH supervisors and managers shall educate staff on reasonable action or mitigation regarding incident response and may aid in problem-solving.
- E. For reportable incidents involving patients (i.e., incident reports with patients listed as “subject”), an RN must assess the involved patient(s) when it is safe to do so and document the assessment in the Electronic Health Record. This assessment should consider elements appropriate to the nature of the incident, such as physical and psychological safety, access to prohibited items, and risk for recurrence.
- F. In addition to an incident report, staff should report incidents as directed within applicable policies as listed below.
  - 1. Staff injuries must also be reported using the electronic OSH incident reporting system and per OSH policy 5.012, “Injury or Illnesses Reporting.”
  - 2. A seclusion or restraint incident must be reported per OSH policy 6.003, “Seclusion or Restraint.”

3. Sexual Contact: 6.016 "Sexual Activity Involving Patients"
4. Patient Falls: 6.046 "Fall Prevention Program"
5. An incident of alleged patient abuse must be reported per OSH policy 7.008, "Patient Abuse Allegation Reporting."
6. Found Medication or Contraband: 8.044 "Contraband Prohibited Items Limited Access Items" and 8.019 "Staff Response to Alleged Criminal Acts"
7. Wandering Patients: 8.018 "Unauthorized Leave Events"
8. An incident involving patient-protected health information must be reported per Oregon Health Authority policy 100-014, "Report and Response to Privacy and Security Incidents."

## **II. REPORTING AN INCIDENT**

- A. All OSH Staff with direct knowledge of a reportable incident are responsible for submitting a report documenting their observations as soon as possible and no later than the end of their shift using the designated incident reporting process in place at the time of the event.
- B. Incident reports must include clear and complete information about any injury to staff or patients, including the nature and extent of the injury, if known at the time of reporting.
- C. Staff are also expected to follow any department-specific protocols, which may include more detailed or immediate reporting requirements beyond those outlined in this policy.

## **III. REPORTING EXCEPTIONS**

- A. As an exception, the following reportable incidents shall be reported in the electronic OSH incident reporting system by designated persons only. Designated persons only need to create one incident report for the following reportable incidents. Designated persons are as follows:
  1. Code red – reported by the Director of Safety or designee
  2. Code orange – reported by the Director of Safety or designee
  3. Code yellow – reported by the Director of Security or designee
  4. Code silver – reported by the Director of Security or designee

5. Widespread mechanical system failure (i.e., sallyport or door locking failure) – reported by Director of Facilities or designee
6. Widespread technology system failure (i.e., phone or network outage) – reported by the Director of Technology Services or designee
7. Events that require law enforcement, emergency medical services, or fire service response outside the secure perimeter only; reported by the Director of Security or designee