

SCENARIO 7 | MEDICAL, DENTAL, BEHAVIORAL HEALTH, AND OTHER HIPAA-COVERED PRACTICES

# Healthcare: EHR Outage and PHI Breach

A ransomware attack takes the practice's electronic health record (EHR) offline, and patient records may have been taken.

|                         |            |                               |                  |
|-------------------------|------------|-------------------------------|------------------|
| <b>Suggested length</b> | 90 minutes | <b>NIST CSF 2.0 functions</b> | Respond, Recover |
|-------------------------|------------|-------------------------------|------------------|

## Exercise objectives

- Test downtime procedures for patient care
- Practice the HIPAA breach risk assessment and notification timeline
- Coordinate with the EHR vendor and business associates

## Recommended participants

Facilitator and scribe, Executive Sponsor, Incident Commander, IT Lead / MSP, Security Lead / vCISO, Legal / Privacy Counsel, Communications, Finance / CFO. Add the roles named in the discussion questions below. Smaller teams can combine roles; see "Scaling roles to your company size" in the Facilitator Guide.

## Injects

Read each inject aloud, then pause for discussion before moving to the next. Facilitators may add or skip injects to fit the time available.

| # | When                | What happens                                                                                                                                                   |
|---|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Thursday, 7:45 a.m. | Front-desk staff cannot log in to the EHR or scheduling system. Patients are arriving for appointments.                                                        |
| 2 | 9:30 a.m.           | The EHR vendor says your cloud tenant is unaffected, but your on-site server that syncs with it is encrypted, and the attackers claim to have patient records. |
| 3 | Day 3               | Forensics confirms that files containing protected health information (PHI) for about 3,200 patients were copied.                                              |

## Discussion questions by role

| Role                                    | Questions                                                                                                                                                     |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Operations / Business Continuity</b> | <ul style="list-style-type: none"> <li>• How do we see patients today using paper downtime procedures?</li> </ul>                                             |
| <b>Legal / Privacy Counsel</b>          | <ul style="list-style-type: none"> <li>• How do we complete the four-factor breach risk assessment, and what are the HIPAA notification deadlines?</li> </ul> |
| <b>Communications</b>                   | <ul style="list-style-type: none"> <li>• What do we tell patients at the front desk today?</li> </ul>                                                         |

| Role          | Questions                                                                                                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IT Lead / MSP | <ul style="list-style-type: none"> <li>• Which business associates and vendors need to be notified?</li> </ul>                                                                                                                                   |
| Everyone      | <ul style="list-style-type: none"> <li>• What information do we need that we do not have?</li> <li>• Who outside the company must we contact, and do we have their numbers offline?</li> <li>• What would we do differently tomorrow?</li> </ul> |

## Key decisions and good practices to look for

- Activate downtime procedures to protect patient safety
- Notify affected individuals without unreasonable delay and no later than 60 days after discovery
- Notify the U.S. Department of Health and Human Services (HHS); breaches affecting 500 or more people also require media notice in the affected state or jurisdiction
- Review business associate agreements
- Adopt HHS 405(d) Health Industry Cybersecurity Practices

**Hotwash (last 15 minutes):** What went well? What surprised us? Which three action items will we complete in the next 30 days, and who owns each? Record them in the After-Action Report template.

**Document it:** the scribe keeps the Exercise Log (see the Facilitator Guide) so the next exercise builds on this one.

This scenario is fictional and for training purposes. Legal and regulatory references are general information, not legal advice; confirm requirements with counsel.