PatientPartner™

2024

INCIDENT RESPONSE PLAN

www.patientpartner.com

Revision History

Revision Number	Summary of Revision	Revision Author	Date
1	Initial document	Zhichao Han	10/1/2020
2	Update communication policy	Zhichao Han	10/19/2021
3	Update plan with more detailed plan for each response phase	Zhichao Han	1/8/2022
4	Update plan with increased scope	Zhichao Han	2/8/2023
5	Annual Review	Zhichao Han	1/10/2024
6	Update plan with client communication, roles and responsibility	Zhichao Han	2/13/2024

Table of Contents

Purpose

This document describes the overall plan for responding to information security incidents at PatientPartner. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The goal of the Incident Response Plan is to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

Scope

This plan applies to the Information Systems, Institutional Data, and networks of PatientPartner and any person or device who gains access to these systems or data.

Definitions

Event

An event is an exception to the normal operation of IT infrastructure, systems, or services. Not all events become incidents.

Incident

An incident is an event that violates the Information Security Policy or any other PatientPartner policy, standard, or code of conduct; or threatens the confidentiality, integrity, or availability of Information Systems.

Incidents may be established by review of a variety of sources including, but not limited to PatientPartner monitoring systems, reports from staff or outside organizations and service degradations or outages. Discovered incidents will be declared and documented in PatientPartner incident documentation system.

Complete IT service outages may also be caused by security-related incidents, but service outage procedures will be detailed in Business Continuity and/or Disaster Recovery procedures.

Incidents will be categorized according to potential for restricted data exposure or criticality of resource using a High-Medium-Low designation. The initial severity rating may be adjusted during plan execution.

Detected vulnerabilities will not be classified as incidents. PatientPartner employs tools to scan the environment and depending on severity of found vulnerabilities may warn affected users, disconnect affected machines, or apply other mitigations. In the absence of indications of sensitive data exposure, vulnerabilities will be communicated and PatientPartner will pursue available technology remedies to reduce that risk.

Personally Identifiable Information (PII)

For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- State-issued identification card number
- Financial account number in combination with a security code, access code or

password that would permit access to the account

• Medical and/or health insurance information

Protected Health Information (PHI)

PHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium by a Covered Component, as defined in PatientPartner's HIPAA Policy. PHI is considered individually identifiable if it contains one or more of the following identifiers:

• Name

• Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)

• All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89)

• Telephone numbers

• Fax numbers

• Electronic mail addresses

• Social security numbers

• Medical record numbers

• Health plan beneficiary numbers

• Account numbers

• Certificate/license numbers

• Vehicle identifiers and serial numbers, including license plate number

• Device identifiers and serial numbers

• Universal Resource Locators (URLs)

• Internet protocol (IP) addresses

• Biometric identifiers, including finger and voice prints

• Full face photographic images and any comparable images

• Any other unique identifying number, characteristic or code that could identify an individual

Incident Response Phases

The basic incident process encompasses six phases: preparation, detection, containment, investigation, client communication, remediation and recovery.

Preparation

Preparation includes those activities that enable PatientPartner to respond to an incident: policies, tools, procedures, effective governance and communication plans. Preparation also implies that the affected groups have instituted the controls necessary to recover and continue operations after an incident is discovered. Post-mortem analyses from prior incidents should form the basis for continuous improvement of this stage. The tools include:

- Logging for activities on the webserver such as login, restarts, deploys
- Logging for incoming requests
- Ability to control access to production database and have point in time recovery to restore state for debugging purposes
- Ability to reset all passwords effectively and force logouts

Detection

Detection is the discovery of the event with security tools or notification by an inside or outside party about a suspected incident. This phase includes the declaration and initial classification of the incident. Methods of detection include:

- Searching through logs for traces of suspicious behavior
- Using the database to find information about user behavior
- Looking across different systems to collect data to see what actions were taken on the platform

Containment

Containment is the triage phase where the affected host or system is identified, isolated or otherwise mitigated, and when affected parties are notified and investigative status established. This phase includes sub-procedures for seizure and evidence handling, escalation, and communication. The steps for containment include

- Determine which subset of systems is compromised
- Rotate credentials for those systems
- Determine the scope of users affected
- Determine the scope of clients affected
- Notify all users and clients affected by the incident and regulatory bodies as needed

Investigation

Investigation is the phase where PatientPartner personnel determine the priority, scope, and root cause of the incident. This involves

- Examining system logs
- Checking all systems for information
- Backing up point in time production data to see state of the platform

Client Communication

In the event of a data incident, timely and transparent communication with PatientPartner's clients is paramount to maintaining trust and ensuring accountability. PatientPartner will notify affected clients promptly, within 24 hours of identifying the incident. Communication channels will vary depending on the severity and scope of the incident but include email notifications and/or secure messaging through the platform. These communications will provide detailed information about the nature of the incident, including what data may have been compromised, the steps PatientPartner is taking to investigate and mitigate the situation, and any actions clients can take to protect themselves. Additionally, PatientPartner will establish a dedicated support channel staffed by knowledgeable personnel to address client inquiries and provide ongoing updates as the situation evolves.

Remediation

Remediation is the post-incident repair of affected systems, communication and instruction to affected parties, and analysis that confirms the threat has been contained. The determination of whether there are regulatory requirements for reporting the incident (and to which outside parties) will be made at this stage. Apart from any formal reports, the post-mortem will be completed at this stage as it may impact the remediation and interpretation of the incident.

Recovery

Recovery is the analysis of the incident for its procedural and policy implications, the gathering of metrics, and the incorporation of "lessons learned" into future response activities and training.

Specific procedures related to this Incident response plan are documented at the PatientPartner's Policies and Procedures internal site.

Roles and Responsibilities

Outlined below are the roles and responsibilities for the relevant parties when an incident is identified:

Data Protection Officer (DPO)

In the event of a data breach, the data protection officer (DPO) assumes a central role in coordinating the response efforts and ensuring compliance with company policies. The DPO is responsible for initiating the incident response plan, including notifying relevant stakeholders, activating response teams, and overseeing the investigation and remediation process. They liaise with external parties, such as PatientPartner's legal counsel, to fulfill reporting obligations and mitigate potential legal repercussions.

Security Administrations

Security administrators play a crucial role in containing and resolving the incident. They lead technical efforts to identify the cause, scope and impact of the incident, implementing measures to halt unauthorized access and preserve evidence. Security admins collaborate closely with the DPO to assess the severity of the incident, prioritize response actions, and implement security enhancements to prevent future incidents.