



December 13, 2023

Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202

RE: 649016

### **NOTICE OF CYBER SECURITY INCIDENT**

Dear Attorney General,

Prospect Medical Systems ("Prospect") is a delegated provider to Humana supplying administrative services for health care providers that are contracted with Humana. Prospect's parent company, Prospect Medical Holdings ("PMH"), experienced a cyber security incident.

PMH detected unusual activity in its Information Technology ("IT") environment which disrupted the availability of certain IT systems. An investigation was launched with the assistance of a third-party forensics firm. Through their ongoing investigation, unauthorized parties accessed and/or acquired files containing information pertaining to Humana plan members.

#### **What information was involved?**

- First and last name
- Addresses
- Date of birth
- Diagnosis
- Lab results
- Medication
- Health insurance and claims information
- Provider names
- Dates of treatment

#### **What we are Doing:**

Upon learning of the incident, PMH immediately took steps to secure their systems and disconnected from trading partners to prevent any potential downstream impact. To help prevent something like this from happening again, PMH added SentinelOne to work in tandem with Microsoft Defender to guard and/or intercept suspicious activity. PMH also notified the FBI of the incident and enlisted Kroll, third-party forensics firm to help with the investigation.

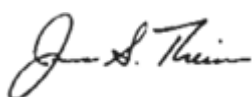
## **What Individuals Can Do.**

Although PMH is unaware of any misuse of any information, they have asked that the impacted individuals remain vigilant. They recommend that individuals regularly monitor medical statements and the explanation of benefits statements that are received to check for any unfamiliar healthcare services.

PMH will begin notifying impacted individuals via first-class mail. A sample template is included with this notification. Humana will promptly report to your office and appropriate law enforcement officials any information that is shared with us that indicates this information has been inappropriately used.

Please do not hesitate to contact me if you have any additional questions regarding this situation.

Sincerely,

A handwritten signature in cursive script, reading "Jim S. Theiss".

Jim Theiss  
Associate VP, Privacy & Ethics  
jtheiss@humana.com  
Humana Inc.

## Exhibit A – Sample Individual Notice Letter



<<Name 1>> <<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

Dear <<Name 1>> <<Name 2>>:

Prospect Medical Holdings, Inc. (“Prospect Medical”) is committed to protecting the confidentiality of the information we maintain. Prospect Medical and its subsidiaries, including Prospect Medical Systems, LLC provides administrative services for health care providers that contract with your Health Plan, [Data Owner]. We are writing to notify you of a data security incident that involved your information. This notice explains the incident, measures we have taken, and some additional steps you may consider taking in response.

**What Happened:** On September 29, 2023, Prospect Medical notified [Data Owner] of a data security incident which involved unusual activity in our Information Technology (“IT”) environment, which was first identified on August 1, 2023. Upon learning of this, Prospect Medical’s IT team took immediate containment action by taking all systems, including servers and workstations, offline. Prospect Medical then launched an investigation with the assistance of a third-party forensics firm.

**What Information Was Involved:** Through our ongoing investigation of the incident, we learned that unauthorized parties accessed Prospect Medical’s IT environment between July 31, 2023 and August 3, 2023 and accessed and/or acquired files containing your information including your [types of information involved will be tailored per patient].

**What We Are Doing:** To help prevent something like this from happening again, we have implemented and will continue to adopt additional safeguards and technical security measures to further protect and monitor our systems.

**What You Can Do:** We recommend you review the statements you receive from your healthcare providers and health insurance plan. If you see any services that were not received, please contact the provider or health plan immediately.

**For More Information:** We deeply regret any inconvenience or concern this incident may cause and take this matter seriously. If you have questions about this incident, please call 888-979-0012, Monday through Friday, 6:00 am – 6:00 pm, Pacific Time, except for national holidays.

Sincerely,

*Michelle Amador*

Michelle Amador  
Compliance and Privacy Officer



2 Emerson Lane  
Suite 200  
Secaucus, NJ 07094  
[www.kroll.com](http://www.kroll.com)

To: Prospect Medical Systems, LLC

From: Kroll Cyber Risk

Date: August 15, 2023

Subject: Prospect Medical Systems, LLC Network Security and Restoration Efforts

---

Kroll was engaged by Baker & Hostetler LLP ("Counsel") on behalf of its Client, Prospect Medical Holdings, Inc. ("PMH"), in response to the recent data security incident. As part of the immediate response, Kroll has employed several cybersecurity and related investigative methodologies, including the use of the Kroll Responder managed detection and response ("MDR") 24/7 monitoring and investigative service. At this point, Kroll has a high level of confidence that containment and eradication for Prospect Medical Systems ("PMS") is complete. Specifically, we note the following material developments:

- PMH and retained Manage Service Provider (MSP), Fenix24, have restored all PMS servers to an off-site data backup taken on July 27, 2023, which was prior to any events associated with this data security incident;
- the remote access method of entry is now off-line;
- all PMS servers and endpoints are being monitored by Kroll Responder, and no threats have been identified;
- the tools associated with malicious and suspicious use during this data security incident were added to the block list within Kroll Responder; and
- in addition to the deployment of Kroll Responder powered by SentinelOne and Defender for Business to PMS endpoints and servers, PMS disabled any devices not showing as protected in SentinelOne, preventing a device not in active use from reconnecting at a later date.

In addition, PMH conveyed to Kroll that they have completed the following high-priority action items:

- performed password changes to all PMS domain accounts;
- blocked known vulnerabilities preventing threat actor's access into the PMH network;
- disabled network connections between sites until security monitoring tools could be deployed;
- blocked known bad software processes within PMH's security monitoring tools;
- enabled ransomware detection and prevention configuration options for antivirus/antimalware software;
- inventory and credential changes for email account access;
- ongoing reconciliation of hardware inventories against Kroll Responder enrollments to ensure comprehensive deployment; and
- Prospect Medical Systems and Kroll collectively attest that the PMS workstations and servers exhibit no remaining indications of compromise.