Search, scale, and protect healthcare data with Elastic

As the company behind the Elastic Stack (Elasticsearch, Kibana, Beats, and Logstash), Elastic builds solutions that make all types of data searchable and usable in real time, at scale, to enable healthcare organizations to achieve key outcomes:

- Perform data aggregation and analysis to predict and prevent disease outbreak
- Monitor and mitigate real-time threats to protected health information
- Forecast medical staffing, budget, and facility requirements
- Accelerate complex research and development of new drugs and treatments
- Detect medical insurance fraud and abuse of benefits programs
- Facilitate rapid national response to current and future medical emergencies
- Safeguard patient data from malware, ransomware, and advanced attacks

Challenges and opportunities for federal healthcare organizations

Federal healthcare organizations manage everything from research and discovery data to pharmaceutical regulation and the development of new treatments for 24 million veterans. While the complexity and scale of healthcare data can be daunting, combining existing data and expertise with advanced search and protection capabilities can deliver timely, trusted results that will lead to medical breakthroughs and improved patient outcomes.

Because Elastic enables near real-time, flexible, and secure advanced analytics, users can leverage all their data for analysis — structured (files), semi-structured (packet capture or PCAP), and unstructured (full text). Most legacy tools cannot analyze unstructured data. Elastic accelerates the search process by making data immediately available for analysis, unlike alternate approaches that index data only upon request.

Scalable, flexible data handling

Global medical and health insurance providers use Elastic in enterprise applications to ingest, search, and analyze multiple data types and formats because it delivers the following:

- Advanced, highly scalable search capabilities
• Fast, flexible, and cost-effective data analytics
• Real-time monitoring and optimization of infrastructure operations
• Data security for Protected Health Information (PHI) and HIPAA requirements

Tools that scale with growing data volumes are essential for healthcare organizations, regardless of the agency or business mission. Elastic enables healthcare providers to manage petabytes of data efficiently and effectively. Query result times can be reduced from the hours and minutes required by legacy technologies to just seconds. With that kind of speed, analysts can do their jobs successfully at scale.

Meeting security and compliance requirements
As attackers continue to evolve techniques that sidestep traditional anti-malware programs, healthcare agencies need to adopt defenses that stay up to date with the latest threats, allow employees to remain productive, and support HIPAA, FISMA, and PCI compliance. Elastic brings endpoint protection and SIEM together in the same experience to streamline how healthcare agencies secure confidential patient information.

Elastic SIEM provides an interactive workspace for analysts to triage events, perform initial investigations, and centralize data across any environment. Elastic Endpoint Security combines prevention, detection, and response into a single autonomous agent. It requires zero training, is built for speed, and stops threats at the earliest stages of attack.

Additionally, all Elasticsearch Service subscription tiers on Microsoft Azure, Google Cloud Platform, and Amazon Web Services are HIPAA compliant.

Replicating private sector success
Global medical and health insurance providers in the private sector use the Elastic Stack to make strides in research, patient care, and operations. These successes can be replicated by federal healthcare agencies.

• Mayo Clinic relies on Elastic to make data meaningful, accessible, and actionable by using patient information collected at point-of-care to develop treatment strategies and improve surgical outcomes.
• Elasticsearch powers the Yale University Department of Laboratory Medicine’s database used by clinicians and researchers to identify novel causes of cancer, potential therapeutic targets, and patient eligibility for clinical trials.
• Merck Research Lab relies on Elastic to support genetics research to streamline drug development, reduce costs, and accelerate time to market for cutting-edge medications.
• UCLA Health leverages Elastic for advanced search capabilities to enable clinicians and technicians to access patient lab results and integrate the data with its electronic medical records.
• Optum, the health services arm of UnitedHealth Group, uses Elastic for cybersecurity data analysis to defend the health information of more than 140 million customers worldwide.
• Cerner, a leading health information and electronic records technology provider, employs Elastic tools to gain insights into infrastructure operations, minimize downtime, and deliver incident-free experiences to more than 27,000 hospitals and medical clinics around the globe.

Extending agency healthcare infrastructures
With an extremely open architecture leveraging RESTful APIs, Elastic components can be used independently or as a full stack depending on the user’s specific requirements. Data and processing can easily be shared with other big data platforms using connectors. Because Elastic can be used on top of and in conjunction with legacy systems and tools, agencies don’t need to rip and replace them.

With no pricing by ingest or host, scaling data into the petabytes is much more affordable with Elastic than with legacy systems. Pay only for what you use.