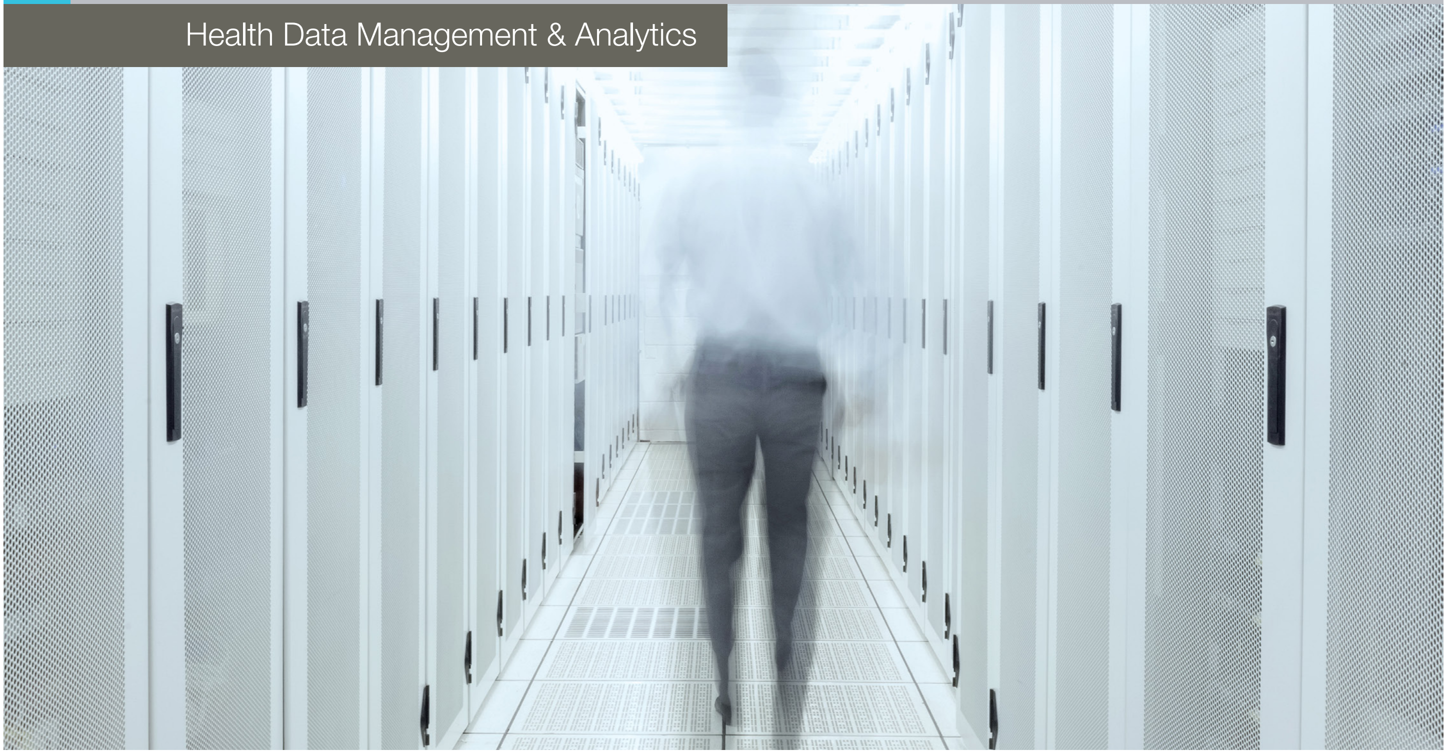
Securing Big Health Data

WHITE PAPER

Health Data Management & Analytics



Securing healthcare data is critical to ensuring privacy, integrity and patient confidentiality. The health sector, like other industries, is becoming increasingly digital and mobile with the adoption of electronic health records, cloud computing, smart phones and tablets. The benefits of adopting modern technologies in the health sector include care and financial efficiencies for both patients and healthcare providers and a more effective use of resources; however, the complexities of protecting patient data have become increasingly significant.

Chronic Condition Warehouse

- One of the largest sources of healthcare patient-linked data
- 315 billion rows of data
- 10 years and 100 tera-bytes of patient-centric data

Virtual Research Data Center

- Remote access to data for approved organizations
- Access to data via a secure virtual desktop

In 2013, for the first time in over a decade, the healthcare sector surpassed the business sector as the industry with the most data security breaches at 43% of all breaches.[1] This fact is relevant to the protection of large data repositories and data warehouses where patient identifiable data is stored, managed and communicated. This paper examines the Chronic Condition Warehouse (CCW) as a world-class example of a highly secure healthcare data infrastructure. The CCW is one of the largest sources of healthcare data in the world, storing 315 billion rows of data, encompassing over 10 years and 100 tera-bytes of patient-centric data. Operated by the U.S. Department of Health and Human Services, Centers for Medicare and Medicaid Services (CMS), CCW provides researchers with Medicare and Medicaid[2] patient data linked across the continuum of care.

[1] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html

[2] The Medicare and Medicaid programs provide health access for certain health populations in the United States. In 2003, legislation called for efforts to improve care quality through better understanding of the population’s health and health utilization. In view of these mandates, the Centers for Medicare and Medicaid Services (CMS) created the Chronic Condition Data Warehouse (CCW) which consists of Medicare and Medicaid data.

Information Security Lifecycle and Chronic Condition Warehouse Data

This lifecycle model ensures CCW's security maturity level is continually being improved with emphasis on constant attention and continual monitoring.

CCW follows a formal information security lifecycle model which is comprised of four interconnecting phases that serve to identify, assess, protect and monitor against patient data security threats. This lifecycle model ensures CCW's security maturity level is continually being improved with emphasis on constant attention and continual monitoring. To this end, CCW security experts enforce compulsory security policies and procedures as the foundation of its security lifecycle model. Each of the four core phases of the CCW information security lifecycle, summarized here within, encompass security policies and mechanisms that ensure rigorous compliance with administrative, physical and technical information system security controls mandated by United States Federal law.

1. Identification Phase – A mature baseline of security used to build upon as new threats and vulnerabilities emerge

The CCW information security program requires that all CMS data and information systems are protected from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft. The security safeguards in place to identify threats are risk-based and business-driven-based on a three-tiered architecture (presentation, application and database layers). A multi-layered Single Sign-On (SSO) solution manages users' access levels across multiple organizations within the CCW environment. CCW has a mature baseline of security that is used to build upon as new threats and vulnerabilities emerge. As CCW resources such as servers, routers, firewalls and applications are examined, vulnerabilities are identified and necessary refinements made for each resource in the assessment phase.

The CCW information security program requires that all CMS data and information systems are protected from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft.

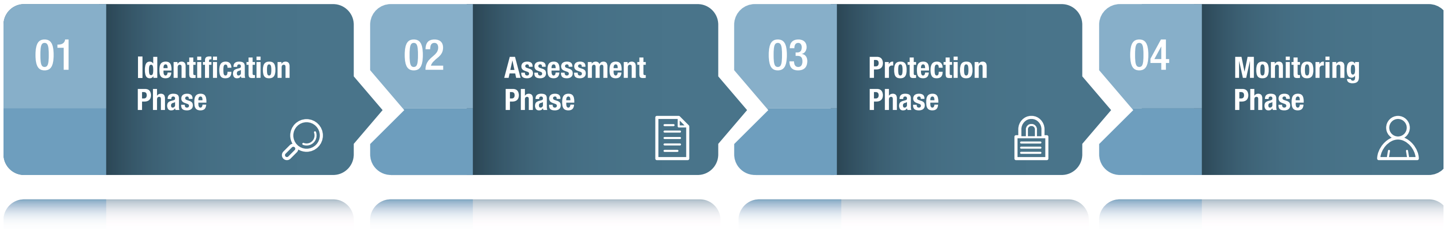
2. Assessment Phase – If the web server was compromised, the data would remain isolated and protected

CCW's three-tiered architecture uses network controls such as firewalls to isolate the presentation layer and the application layer, and then again between the application layer and the database layer. The physically separated tiers increase security because it adds an extra level of indirection between the web server (presentation tier) and the data (database tier). No direct route from the web server to the database exists. If the web server was compromised, the data would remain isolated and protected.

Access to the CCW environment is tightly controlled. Access is granted only after a new requester's identification and authorized approvals are verified and each user completes security awareness training including an acknowledgment of the CCW User Agreement. Even then, access is granted only for the performance of stated tasks approved through the organization's specific Data Use Agreement. CCW's access management solution combined with strict access requirements for new users and regular account attestations fulfills the promise of both user convenience and strong security access control.

CCW's access management system provides SSO functionality which maintains access level security and access control. The CCW access management system utilizes an extensive list of directories and databases as a central repository for user credentials, application logon templates, password policies and client settings to verify that each user's identification, authentication and control access levels are appropriate. This level of scrutiny protects CCW's users, applications and sensitive data.

Core Phases of the Chronic Condition Warehouse


01 Identification Phase

02 Assessment Phase

03 Protection Phase

04 Monitoring Phase

3. Protection Phase – Mitigating risks identified during the assessment phase

The protection phase is sometimes referred to as the “mitigation” phase, because the objective is to mitigate any risks identified during the assessment phase. The focus of this phase is to configure and update each system and network component so that its security is strengthened and complies with CCW policy. This process helps eliminate or decrease the risk level of vulnerabilities. All changes to the CCW environment are managed by a formal change control process that includes utilizing a development and test environment to ensure implementation to production is a controlled managed process.

4. Monitoring Phase – Security compliance and verification

Security compliance and verification is the primary objective of the monitoring phase. To ensure CCW’s established security environment for servers, firewalls and routers remains in place and unchanged, many security application tools are utilized by the CCW security team. The Intruder Detection System monitors the network for intruder attacks while Policy Compliance tools monitor and measure the status of security across the enterprise. These tools provide the CCW security team with detailed information on the configuration of servers, databases or network components and evaluate the configuration against security policies.

The CCW’s Information Security lifecycle ensures the confidentiality, integrity and availability of the CCW environment. There are sets of rules which limit users’ access to the CCW’s environment and information ensuring data confidentiality. Access to the information is guaranteed once the user’s identity has been verified and authorized.

The CCW’s Information Security lifecycle ensures the confidentiality, integrity and availability of its environment, and sets of rules limit users’ access to the CCW’s environment and information, ensuring data confidentiality.

Chronic Condition Warehouse Encryption Process for Data Dissemination

In order to securely transfer CCW data to requested Data Use Agreement approved organizations, the CCW analytics team prepares the requested data files by using a file encryption solution with Self-Decrypting Archive (SDA) method. The SDA method builds a compressed, encrypted, password-protected data file using a federally-approved encryption algorithm. This SDA method establishes a data file that is unreadable and safe to transfer. Upon receipt, only authorized users are able to decrypt the SDA file via a password transmitted separately to the end user to ensure that unauthorized access to the data is not possible. The unique patient-identifiable fields are also encrypted using a cipher prior to delivery of the data files. A unique cipher is requested and established for each patient’s data file, enabling researchers to follow patients’ care over the course of years.

Information-driven healthcare also empowers patients with access to their personal health data enabling them to make informed decisions about their own care and manage their long-term chronic conditions effectively.

Virtual Research Data Center and the Chronic Condition Warehouse – Secure virtual access to data

In November 2013, CMS launched the Virtual Research Data Center (VRDC) as a module within CCW which provides a remotely accessible analytics environment with secure virtual access to the most comprehensive, up-to-date Medicare data sets available in the CCW. To improve healthcare quality and efficiency, the VRDC provides researchers with access to data in a more timely manner and via a variety of tools to analyze the data. It also provides greater security controls for data access restrictions and protection of privacy data. In the VRDC, sensitive information about individual patients never leaves the CCW data environment and researchers access the data through a secure virtual desktop. The VRDC provides researchers with several advantages including lower costs to access the Medicare data, avoiding the requirement to maintain expensive data infrastructures. In the past, CMS shipped data to researchers on an annual basis, however, the VRDC enables researchers to access data significantly faster by removing the time consuming barriers presented by physical data delivery. Researchers also benefit from the ability to refresh their data routinely. The VRDC provides greater security around sharing data with research agencies. Under the VRDC model, sensitive individually-identifiable information about patients never leaves the CMS data environment, safeguarding against accidental breaches or unauthorized use of the data.

General Dynamics Health Solutions and the Chronic Condition Warehouse

General Dynamics Health Solutions developed and maintains the CCW and VRDC and is an experienced integrator of complex health systems which empower healthcare providers with secure access to electronic information. We work with organizations to exchange and share health data in meaningful ways, enabling data to become interconnected information that plays a critical role in improving the quality of care and balancing the cost of healthcare delivery.

Our end-to-end health solutions – which expand insight, improve outcomes, drive efficiency and reduce risk – include:

- **Health Data Management & Analytics**
- Multi-Channel Health Communications
- Health Facility Outfitting & Logistics
- Clinical Staffing & Medical Research Services
- Healthcare Administrative Services
- IT Services & Infrastructure

About General Dynamics Information Technology
As a trusted systems integrator for more than 50 years, General Dynamics Information Technology provides information technology (IT), systems engineering, professional services and simulation and training to customers in the defense, federal civilian government, health, homeland security, intelligence, state and local government and commercial sectors. Headquartered in Fairfax, Va., with major offices worldwide, the company delivers IT enterprise solutions, manages large-scale, mission-critical IT programs and provides mission support services. General Dynamics Information Technology is one of four business units of the General Dynamics Information Systems and Technology business segment.

7645 – 4/1/15

General Dynamics Information Technology is an Equal Opportunity/Affirmative Action Employer – Minorities/Females/ Protected Veterans/Individuals with Disabilities.