THE **HUMAN** FACTOR IN HEALTH DATA SECURITY

Human error represents one of the leading causes of lost or stolen personal health information (PHI). In an industry where data breaches can expose agencies or organizations to millions of dollars in HIPAA fines, class-action lawsuits, reparations, and reputational damage, it is no longer sufficient to rely on technology alone to safeguard sensitive health data.

The average economic impact of each data breach for healthcare providers is **$2.4 million**

Health data security poses an ongoing challenge for government agencies and private sector institutions alike:

Government health data remains a common target of theft and fraud.

Although only **10%** of U.S. health data intrusions access data from government institutions, government data accounts for **40%** of all health records stolen

94% of private healthcare organizations had at least one data breach in the last two years

138% PHI breaches up 138% in 2013

70 70 breaches in January 2014

21 mil 21 million Americans are victims of unauthorized health data disclosure

Data breaches can result from any number of human errors:

- **Connecting** devices through unsecure wireless networks
- **Leaving** portable electronic devices unattended
- **Improper disposal** or mailing of paper documents
- **Failure** to fully implement or update information security protocols
- ***123 **Reusing** passwords on work and personal devices

Healthcare executives list human error among the most frequent cause of lost or stolen PHI

How can government agencies and healthcare providers better safeguard data by reducing human error?

Adopt a **security-centric mindset** when hiring, onboarding, and continually training employees

Encrypt all laptops, desktops, and mobile devices to mitigate the damage done by lost or stolen property

Automate systems to control virtual and physical access to sensitive data

Conduct frequent **audits and risk assessments** in compliance with FISMA and HIPAA protocols

Government Business Council

ABOUT GBC
Government Business Council (GBC), the research arm of Government Executive Media Group, is dedicated to advancing the business of government through analysis and insight. GBC partners with industry to share best practices with top government decision-makers, understanding the deep value inherent in industry's experience engaging and supporting federal agencies.

GENERAL DYNAMICS
Information Technology

ENABLING CONNECTIONS. APPLYING EXPERIENCE. IMPROVING OUTCOMES.
General Dynamics Information Technology helps our clients improve care quality for their stakeholders by enabling better ways to connect. Applying extensive health and health IT expertise for today's healthcare challenges, we provide innovative solutions that help you analyze big health data, enable payment reform, manage population health, modernize IT infrastructure and systems, exchange health information (HIE), fight healthcare fraud, waste, and abuse. Learn more about our work at www.gdit.com/health.

Sources:

FierceHealthIT, Security Ruling Could Spell Double Trouble for Hospital CIOs
Redspin, 2013 PHI Breach Report.
HITRUST, A Look Back: U.S. Healthcare Data Breach Trends
Ponemon Institute, Third Annual Benchmark Study on Patient Privacy & Data Security
Information Security Media Group, Healthcare Information Security Today: 2013 Outlook