Elevated Heart Rates: EHR and IT Security

March 8, 2011

Study Intent and Purpose

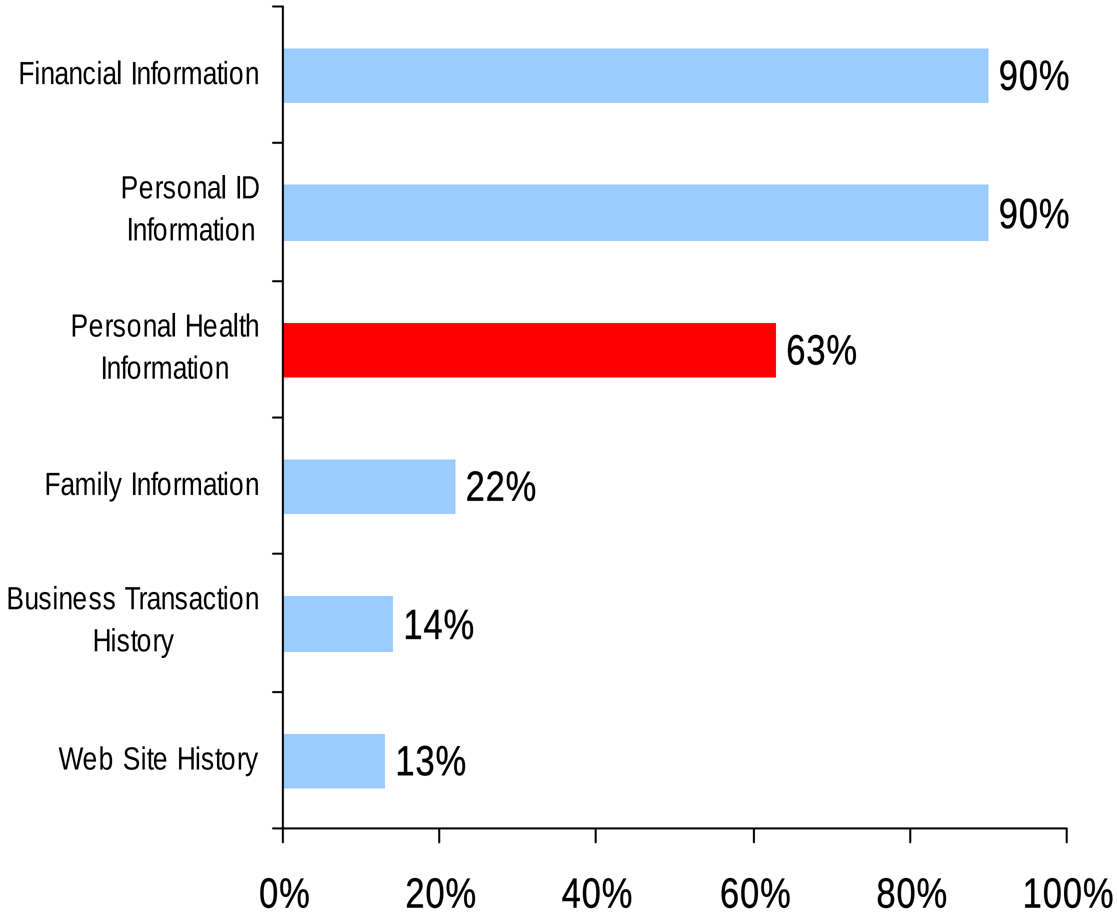
Many healthcare organizations are driving to implement electronic health records (EHRs) during 2011 in an effort to capture early-adoption incentive payments. Patients have a stake in this transition. As more information becomes digitized, new processes, technologies and policies will be required to protect it. EHRs are not inherently less secure, but they do have different security requirements.

This report outlines patient perceptions of IT security in healthcare, and patient requirements for the protection of their personal information, including:

- Who patients trust to view and manage their personal information
- What patients consider to be their personal information and how they think EHRs will affect the privacy and security of that personal information
- How patients will likely respond to security breaches
- What steps healthcare organizations should take to prepare for the new information technology security requirements created by the transition to EHRs

Defining and Prioritizing Personal Information

What personal information do you believe is the most important to keep private and secure? (top three)



Financial Information
Credit card numbers, bank account numbers, credit score, etc.

Personal ID Information
Birth date, Social Security number, physical address, etc.

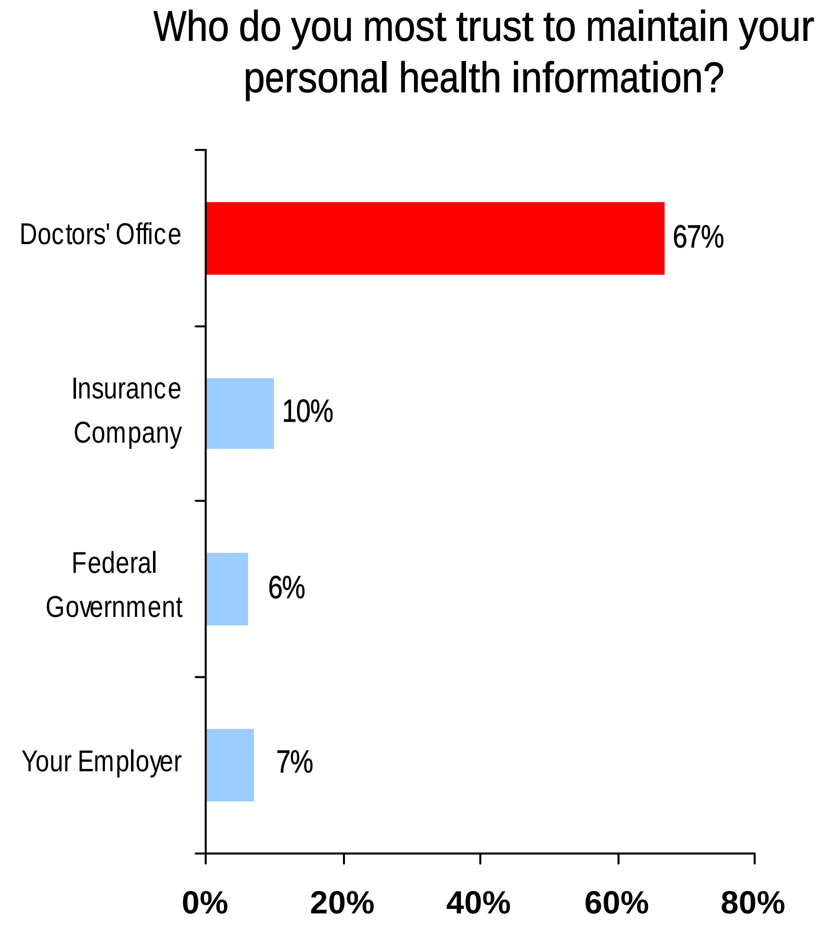
Personal Health Information
Treatments, diagnoses, prescriptions, types of doctors, etc

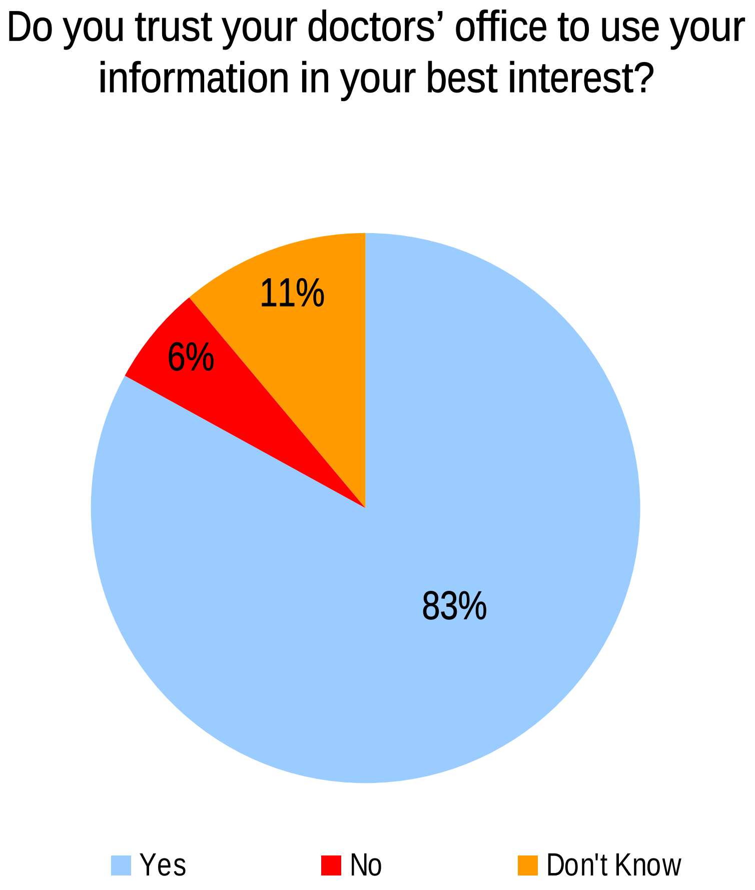
Family Information
Relatives' names, relationships and ages, physical addresses, etc.

Business Transaction History
Purchases, buying history, amounts, discounts, etc.

Web Site History
List of Web sites visited on home and work computers

Patients Trust Their Physician and The Doctors' Office





In addition, 89 percent of respondents have "complete" or "some degree" of trust in their hospital/outpatient facilities to protect their personal information.

Cite as: CDW Healthcare Elevated Heart Rates: EHR and IT Security Report

New Era; New Requirements – More Information to Protect

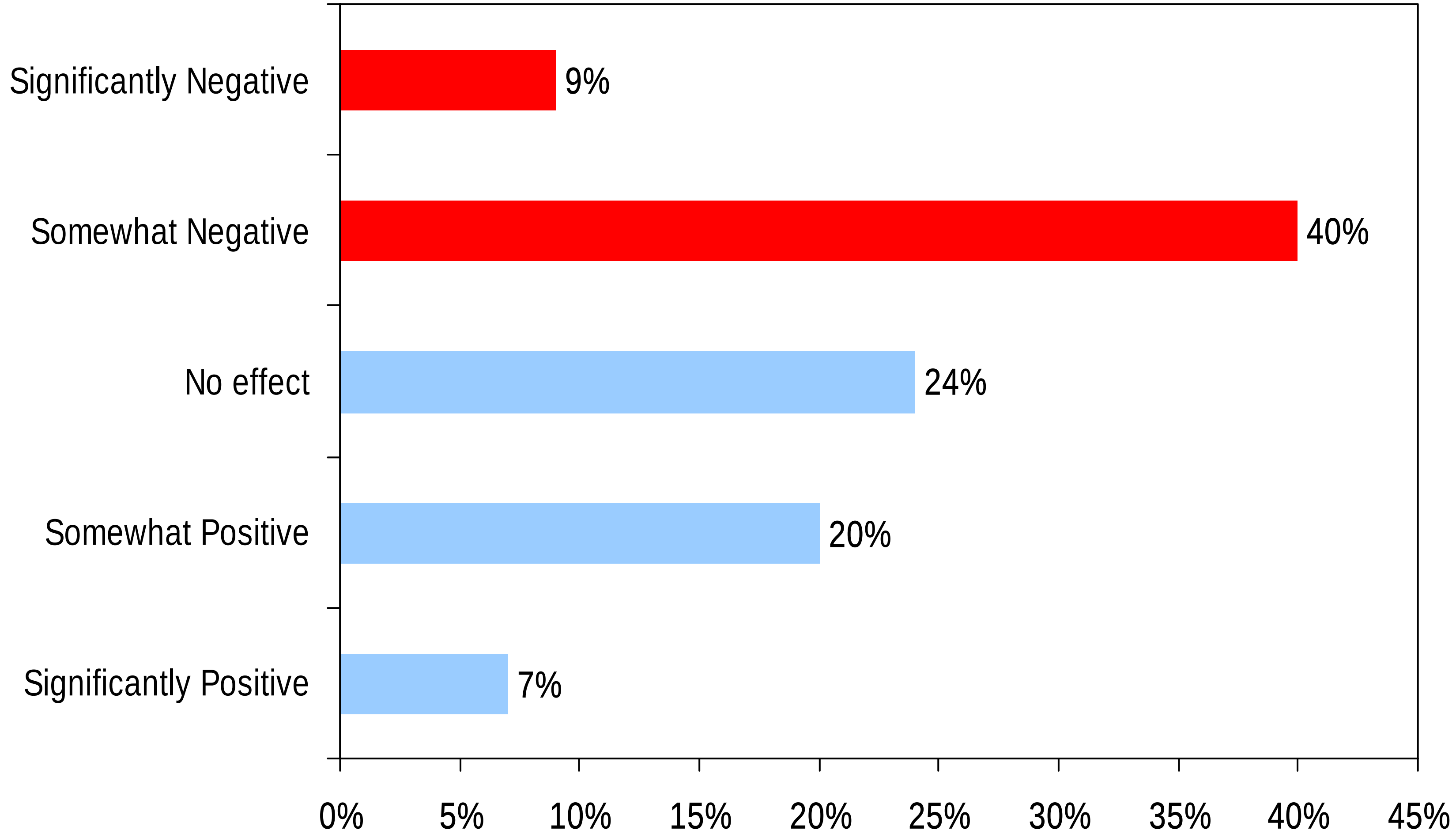
What personal information do you believe that your doctors' office and hospital/outpatient facility are responsible for protecting?

Information Type	Doctors' Office	Hospital/Outpatient Facility
Financial Information	79%	86%
Personal ID Information	91%	93%
Personal Health Information	68%	71%
Family Information	94%	94%
Business Transaction History	1%	1%
Web Site History	1%	1%

Cite as: CDW Healthcare Elevated Heart Rates: EHR and IT Security Report

Elevated Heart Rates – Patients See Risk in EHRs

What impact do you believe that electronic health records (EHRs) will have on the privacy of your personal information and health data?



HEALTHCARE

Elevated Heart Rates – Top Concerns

Which of the following uses of your personal health information concerns you the most?

Concern	%
Your personal health information being available to anyone on the internet	35%
Criminals using personal health information for blackmail or ID theft	22%
Employers reporting personal health information to manage benefits and compensation	12%
Companies using personal health information to make hiring decisions	10%
I am not concerned about any use of my personal health information	10%
Companies using personal health information to develop marketing programs	9%

24%

Of survey respondents have concerns about even trusting themselves enough to access their own health data

Elevated Heart Rates – Patients Have Good Reason for Concern

STOLEN

ID 3306: Stolen Laptop
Date: 12/23/10 Records Lost: 3,159
Organization: Clinic
Location: Minnesota

LOST

ID 3286: Lost Memory Card
Date: 12/13/10 Records Lost: 2,284
Organization: Medical Center
Location: Mesa, AZ

STOLEN

ID 3293: Stolen Laptop
Date: 12/20/10 Records Lost: 3,288
Organization: Health System
Location: Fitchburg, WI

Source: datalossdb.org

Elevated Heart Rates – Severe Symptoms

Many physician practices are not prepared to handle electronic patient data securely, CDW Healthcare found during a 2010 national survey of 200 physician practices. The survey revealed critical gaps in the IT security profile of the average physician practice:

30%

Of surveyed physician practices do not have basic anti-virus software protection

34%

Of surveyed physician practices do not use firewalls

Source: CDW Healthcare Physician Practice EHR Price Tag

Breach My Privacy; Lose My Trust (And My Money)

Fully, 50 percent of survey respondents indicated that a business/organization had notified them about the potential or actual loss or theft of their personal data. Of those customers whose security had been breached:

9%	Sever their relationship with the offending business or organization
12%	Reduce the amount of money that they spend with the offending business or organization
12%	Maintain the relationship, but no longer trust the offending business or organization

New Requirements – Real Consequences for Data Loss

The Health Information Technology for Economic and Clinical Health Act ("HITECH Act") provisions of the American Recovery and Reinvestment Act of 2009 ("ARRA") put real teeth into the enforcement of privacy protections required by the Health Insurance Portability and Accountability Act (HIPAA). Notably:

- **Enforcement by State Attorneys General:** Under the HITECH guidelines, state attorneys general may now bring action against healthcare organizations on behalf of citizens for privacy breaches. Attorneys General from Connecticut and Indiana have already filed suits

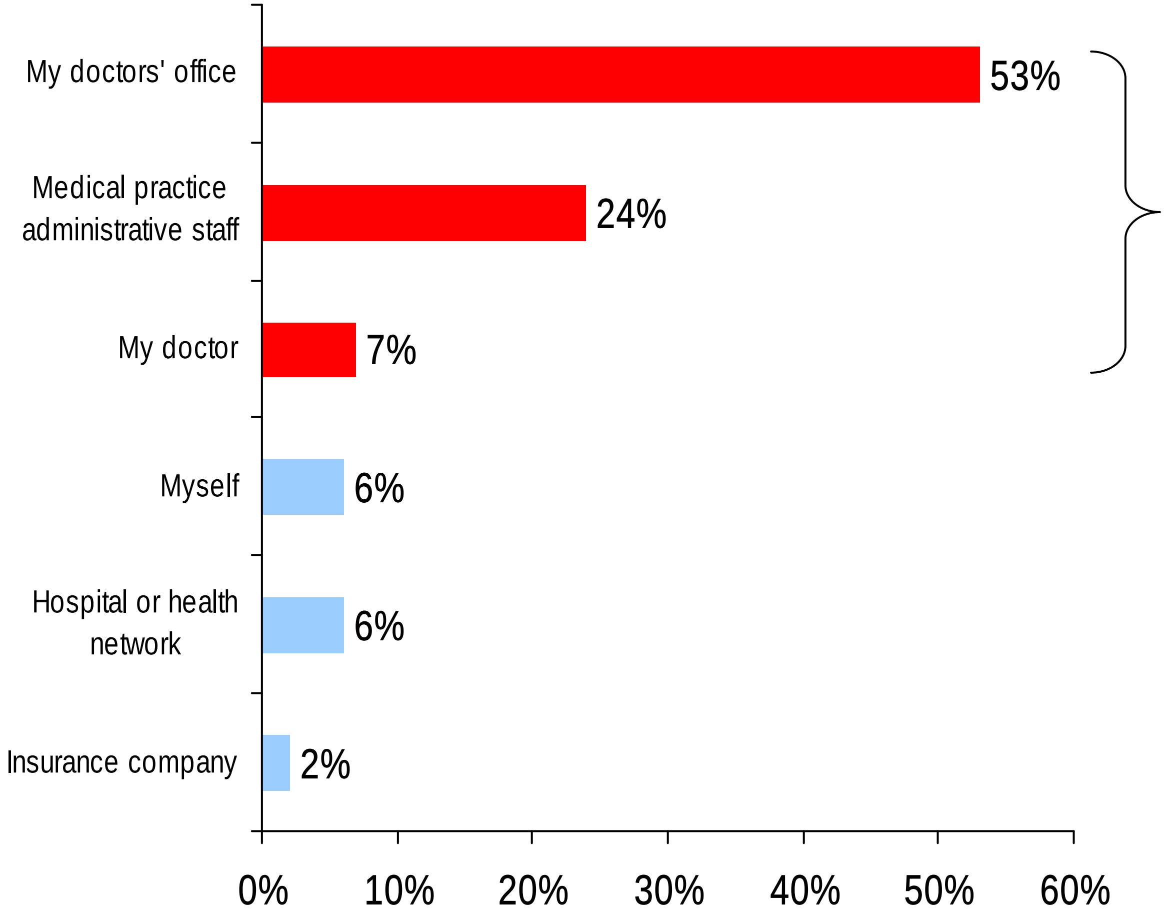
- **Substantial Civil Fines:** For minor, accidental infractions, penalties start at $100 per violation with a limit of $25,000 per year. For willful neglect of uncorrected problems, the penalties start at $50,000 per violation with a ceiling of $1.5 million

- **Criminal Liability:** Individuals who obtain or disclose personal health information maintained without authorization may be subject to criminal liability

Source: U.S. Department of Health and Human Services

Patients Hold Doctors Responsible for Data Protection

Who do you hold primarily responsible for the privacy and security of the information that you provide at your doctors' office?*



84%

Of surveyed patients hold their doctors’ offices as primarily responsible for protecting their data

*2 percent selected “other”

Cite as: CDW Healthcare Elevated Heart Rates: EHR and IT Security Report

Conclusions – New Requirements for a New Era

- Patients hold doctors' offices directly responsible for patient data. 80 percent of respondents cite the doctors' offices in general or someone at the office as responsible for the protection of their personal data

- Patients trust their doctor's office: 83 percent of respondents trust doctors to use their data in their best interest and 67 percent trust physician practices to protect their data

- That said, patients have concerns about EHRs. 49 percent of respondents believe EHRs will have a negative effect on their personal information and health data

- Based upon data from the CDW's Physician Practice EHR Price Tag Report, some practices are not ready to protect electronic patient data: 30 percent do not use anti-virus software and 34 percent do not use firewalls

Recommendations – A Healthy IT Security Lifestyle

With the new era of EHRs comes a broad new set of requirements for physician practices, hospitals and health networks. These organizations must be prepared to protect vast new stores of information against theft, loss and misuse. To prepare, healthcare organizations should:

- Execute an IT Security Assessment: Many healthcare organizations do not know the current state of their IT security infrastructure. Fewer still know what constitutes an adequate profile. Healthcare organizations need to work with a trusted partner to secure a baseline understanding of what their security profile looks like today
- Start with the Basics: Notably, 30 percent of physician practices state that they do not use antivirus software and 34 percent do not use network firewalls. At the absolute minimum, healthcare organizations need to immediately implement steps to meet reasonable security standards
- Protect Your Investment: As healthcare organizations consider the transition to EHRs, they have the perfect opportunity to implement IT security practices tailored to their solution. This not only protects a sizable investment in technology, but also ensures that as patient data goes digital, security protections are already in place
- Start Now; Reassess Often: IT security is not a one-time fix. Though the EHR transition is a perfect time to initiate tighter IT security controls, all healthcare organizations need to consider their IT security profiles and should consider conducting an assessment at least once a year

A National Survey

- Between January 24 and January 31, 2011 CDW Healthcare surveyed 1,000 adults in the United States about the security and privacy of their personal information
- All respondents have been to both a doctors' office and a hospital/outpatient facility during the previous 18 months
- Age and gender distribution of the sample population matches that of the overall U.S. population

Thank you.

For all media questions and inquiries, please contact:

Kelly Caraher
CDW Healthcare
847-968-0729
kellyc@cdw.com

Andrew H. LaVanway
O'Keeffe & Company
703-628-2503
alavanway@okco.com