

HOW SECURE IS YOUR DATA?



ASSESSING AND MITIGATING RISKS

in the Digital Health Era



STORING HEALTH DATA

Last year, **9 OUT OF 10** office-based physicians noted that they'd adopted Electronic Medical Records (EHR).

Since 2008, EHR adoption rates have doubled from **42%** to **87%**.

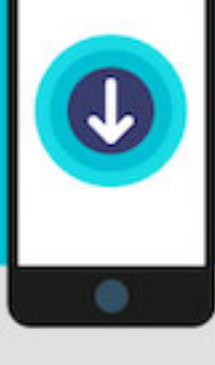
Across all the hospital types roughly **90%** of hospitals have EHR technology.

42% 2008

87% 2016

50%

It is estimated that by 2018, half of the **3.4 billion** smartphone and tablet users will have **health apps** downloaded.



Americans use mHealth for



66% of Americans use a mobile app to **manage health related issues**.



45% of Americans use mHealth for **tracking symptoms**.



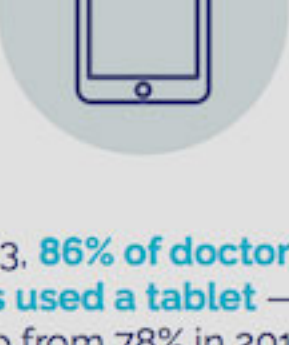
46% use it for **medication reminders**.



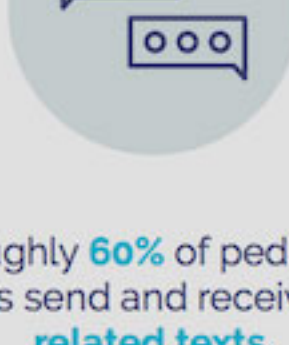
61% use it to **communicate with their doctors**.



Doctors are **250% more likely** to own a tablet than average consumers.



In 2013, **86% of doctors and nurses used a tablet** — that's up from 78% in 2012.



Roughly **60%** of pediatric doctors send and receive **work related texts**.

DIGITAL STORAGE METHODS



TIERED STORAGE

Involves a great deal of **networking**. Data is packed away within a range of different media all based on availability, recovery requirements and performance.

For example, data that could be used for restoration in the event of corruption could be stored locally (on-site servers or backup hard drives), and data not needed immediately could be archived remotely via the cloud.



STORAGE AREA NETWORK (SAN) STORAGE

A **high-speed network** that connects multiple servers to different storage devices.



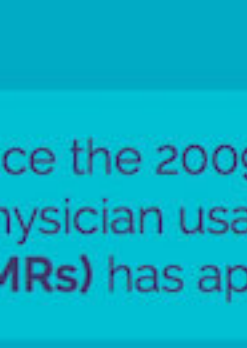
CLOUD STORAGE

Data is stored within **remote servers**, and it's accessed via the Internet.



PICTURE ARCHIVING AND COMMUNICATION SYSTEM (PACS)

A health care technology for long-term and short-term **storage of medical images**. Retrieval, management and distribution are all tied to the system.



HYBRID STORAGE METHODS

Hybrid storage involves using **multiple storage methods** to secure data. Some data is stored remotely via the cloud, while other key data is stored locally in servers.

2x

In the time since the 2009 HITECH Act, the rate of office-based physician usage of **electronic medical records (EMRs)** has approximately **doubled**.

HEALTH DATA RISKS

One study noted that roughly

90%

of health care organizations experienced a **data breach** in the last two years.



there were a total of

253 health care breaches

last year, resulting in a combined loss of well over

112 million health records.



INDIVIDUALS AFFECTED BY HEALTH INFORMATION BREACHES, 2015

Hacking/IT incident	Improper disposal	Loss	Theft	Unauthorized access
111,812,172	82,421	47,214	740,598	572,919

Data breaches cost the health care industry roughly **\$5.6 BILLION** each year.

1 in 3 U.S. citizens had their health data compromised by a series of breaches last year.

The first six months of 2016 averaged **25.3 breaches each month**.

The second half of the year featured an average of **39 breaches each month**.

A 55 PERCENT INCREASE



MAJOR LEAKS include the

- 1** **Premiera Blue Cross hack that affected 11 million customers.**
- 2** **Anthem Blue Cross hack, which impacted 78.8 million records.**

HOW TO PROTECT PATIENTS' DATA



1

Conduct an annual **HIPAA security risk analysis** to ensure that **all storage tools are secure**.



2

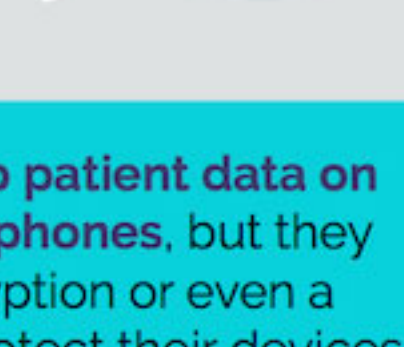
All data-at-rest and all mobile devices — including tablets — **should be encrypted**.

From 2009 to 2014, the theft (or accidental loss) of unencrypted devices contributed to a **third of all major breach incidents**.



3

Physicians and nurses need to understand how to store and send data securely. In other words, **use decent passwords, log out of networks** when finished and **avoid using personal devices**.



22.3% of all health IT users actually **share their passwords** with other users.

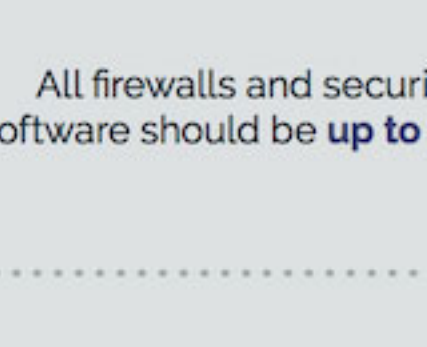
14%

of doctors **keep patient data on their personal phones**, but they don't use encryption or even a password to protect their devices.



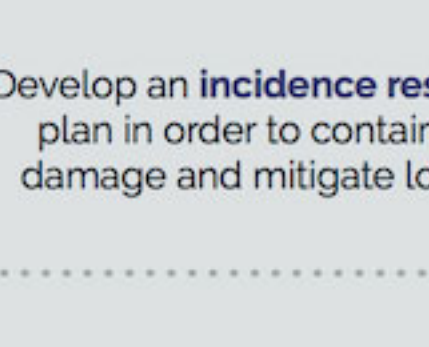
4

All networks and servers should have **remote wiping** or remote disabling enabled.



5

All firewalls and security software should be **up to date**.



6

Develop an **incident response plan** in order to contain the damage and mitigate losses.

7

Develop a security strategy that's customized for the particular data an organization stores (e.g. Social Security information).



healthinformatics.uic.edu

SOURCES

Chapter 1

<https://dashboard.healthit.gov/quickstats/pages/physician-electronic-adoption-trends.php>
<https://dashboard.healthit.gov/quickstats/pages/FIG-Hospital-EHR-Adoption.php>
https://www.healthcatalyst.com/success_stories/integrating-source-marts-into-a-healthcare-data-warehouse/
<http://www.beckershospitalreview.com/healthcare-information-technology/16-statistics-on-physicians-at-work-texting-habits.html>
<http://www.beckershospitalreview.com/healthcare-information-technology/6-statistics-on-the-use-of-mhealth.html>

Chapter 2

<http://www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data>
<http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#5aa893b27fd5>
<http://www.beckershospitalreview.com/healthcare-information-technology/16-latest-healthcare-data-breaches-security-incidents.html>
<https://www.cnbc.com/2016/08/05/why-2016-could-be-banner-year-for-health-care-data-breach-fines.html>
<http://www.healthcare-informatics.com/news-item/cybersecurity/report-healthcare-data-breaches-continue-alarming-pace-second-half-2016>
<https://dashboard.healthit.gov/quickstats/pages/breaches-protected-health-information.php>
<http://www.modernhealthcare.com/article/20161217/MAGAZINE/312179841/the-2016-year-in-review-information-technology>
<http://hitconsultant.net/2016/01/28/hackers-caused-98-of-healthcare-data-breaches/>

Chapter 3

<http://www.healthcareitnews.com/news/6-best-ways-protect-against-health-data-breaches>
<https://www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/>
<http://www.healthcare-financenews.com/blog/new-proactive-not-reactive-protecting-healthcare-data>
<http://www.healthcare-informatics.com/article/new-approach-protecting-healthcare-data-security>
<http://www.healthcarebusinessstech.com/best-practices-to-secure-healthcare-data/>
<https://securityintelligence.com/why-is-medical-data-so-difficult-to-protect/>
<http://www.beckershospitalreview.com/healthcare-information-technology/data-breach-threat-22-of-healthcare-workers-share-their-passwords.html>
<https://www.scmagazine.com/report-14-of-doctors-keep-patient-data-on-cell-phones-dont-use-password/article/528774/>

Additional Sources:

<http://www.cio.com/article/3092324/big-data/4-reasons-why-healthcare-needs-a-digital-code-of-ethics.html>
<http://www.ahrq.gov/research/findings/final-reports/omracereport/reldata5.html>
<https://www.practicefusion.com/health-informatics-practical-guide/>
<https://www2.idexpertscorp.com/blog/single/mobile-devices-expanding-threats-to-healthcare-data>
<http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/default.htm>
<https://www.nahdo.org/about>
<http://www.healthit.techtarget.com/essentialguide/Healthcare-data-storage-options>
<http://www.hrsa.gov/quality/toolbox/methodology/performanceimprovement/>