# Comparative Study of HIM Professionals Comprehension and Use of Data Protection on Mobile Devices

Save to myBoK

By Julie M. Wulf Plimpton, MSHI, RHIA, CPHI

As smartphone use continues to grow, these devices are often used to access an individual's private information. American mobile device users spend, on average, five hours of their day communicating or accessing information on their smartphones. Approximately 69 percent of that time is spent in apps. Recent figures show healthcare apps have helped boost that percentage, as more than 50 percent of smartphone users gather health-related information on their phones, while 80 percent of physicians use smartphones and medical apps.

In research presented at Dakota State University's (DSU's) Research Day event in April, investigators at DSU described their survey of health information management (HIM) professionals using a Likert model survey on AHIMA's Engage member portal. The survey asked questions related to age, gender, job title, and personal information use on smartphones. The goal was to evaluate the level of security HIM professionals have on their smart devices.

## Study Background

Smartphones are used in everyday life for writing and sending emails, banking, and communicating with healthcare providers. As smartphones replace personal computers, large volumes of sensitive data are now stored and processed on these devices, including contacts, emails, photos, and videos. This makes smartphones an attractive target for hackers, particularly in often-unintended installation of malicious codes.

The US Department of Health and Human Services' (HHS') Office for Civil Rights (OCR) recognized that mobile devices—including cell phones, tablets, and laptops—are increasingly found in many work environments, including healthcare organizations. While the use of mobile devices in the workplace can increase productivity in simple, manageable ways, there are several potential risks when mobile devices are used to create, receive, maintain, or transmit electronic personal health information (ePHI).

## Results and Discussion

The public is not very informed about the need for additional security levels beyond password and biometrics on the home screen, according to results of the DSU survey. Individuals are not sufficiently protecting their PHI from outside intruders since they are not aware of the need for additional security, which can include antivirus software and exclusive use of secure Wi-Fi networks. The survey also indicated that 56.4 percent of participants did not use antivirus programs on their smartphones but used other methods of security.

Of the 39 returned surveys (not a full representation of the population surveyed), 97 percent of the responses—in a reflection of AHIMA's demographics—were from female participants. Other findings are outlined on Table 1.

**Table 1 - Survey Demographics**
This Survey asked Engage survey participants about their age, gender, and job title.

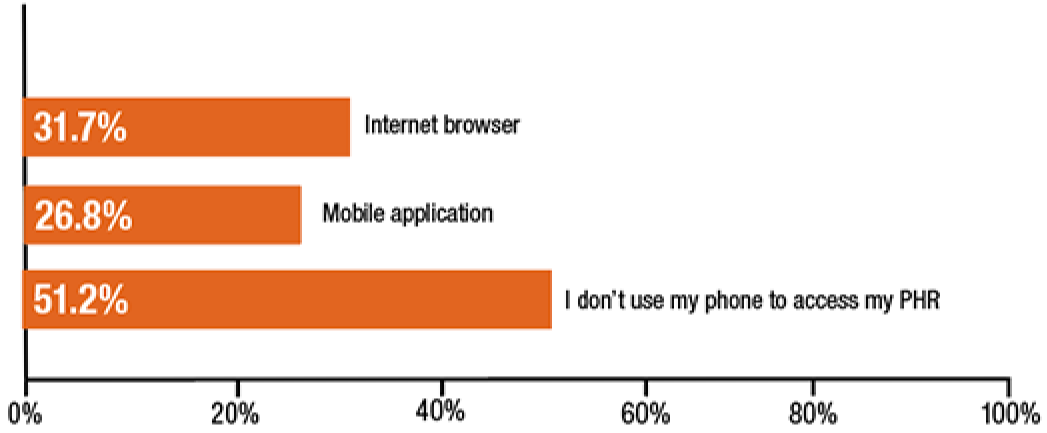
| Parameter | Range | Percentage |
|---|---|---|
| Age | 18-29 | 5% |
| | 30-39 | 3% |
| | 40-49 | 13% |
| | 50-59 | 46% |

| | | |
|---|---|---|
| | 60-69 | 25% |
| | 70-79 | 8% |
| Gender | Male | 3% |
| | Female | 97% |
| Job Title | Administration | 0% |
| | Physician | 2% |
| | Nurse | 0% |
| | HIM | 77% |
| | IT | 5% |
| | Ancillary | 2% |
| | Coder | 2% |
| | Consultant | 2% |
| | Educator | 2% |
| | Privacy/Compliance | 2% |
| | Risk Manager | 2% |
| | HIM Auditor | 2% |
| | Retired HIM | 2% |

## Survey Results

In response to the question “What type of antivirus software do you have on your phone, if any?” more than half of those surveyed indicated that they do not have antivirus software on their smartphone, leaving them vulnerable for hacking.

**Graph 1 - PHR Use on Smartphones**
This question asked respondents about how they accessed their health data on their phones.



## Room for Additional Education

As indicated in this study, healthcare administrative professionals are aware of the need to protect the data on their smartphones with some level of security. However, there is room for additional education on the best ways to protect personal and confidential information on smartphones from hackers.

Potential next steps include conducting additional research that includes a systematic review or meta-analysis of all related published literature.

### Notes

1. Perez, Sarah. "U.S. consumers now spend 5 hours per day on mobile devices." Tech Crunch. March 3, 2017. https://techcrunch.com/2017/03/03/u-s-consumers-now-spend-5-hours-per-day-on-mobile-devices/.
2. Becker's Health IT & CIO Report. "Report: 80% of Physicians Use Smartphones, Medical Aps." https://www.beckershospitalreview.com/healthcare-information-technology/report-80-of-physicians-use-smartphones-medical-apps.html.
3. US Department of Health and Human Services. "Summary of the HIPAA Privacy Rule." https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.
4. National Institute of Standards and Technology. "Guidelines for Managing the Security of Mobile Devices in the Enterprise." June 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

Julie Wulf Plimpton (Julie.wulfplimpton@dsu.edu) is an assistant professor at Dakota State University.

**Article citation**:
. "Comparative Study of HIM Professionals Comprehension and Use of Data Protection on Mobile Devices" *Journal of AHIMA* 90, no.10 (October 2019): 32-33, 43.