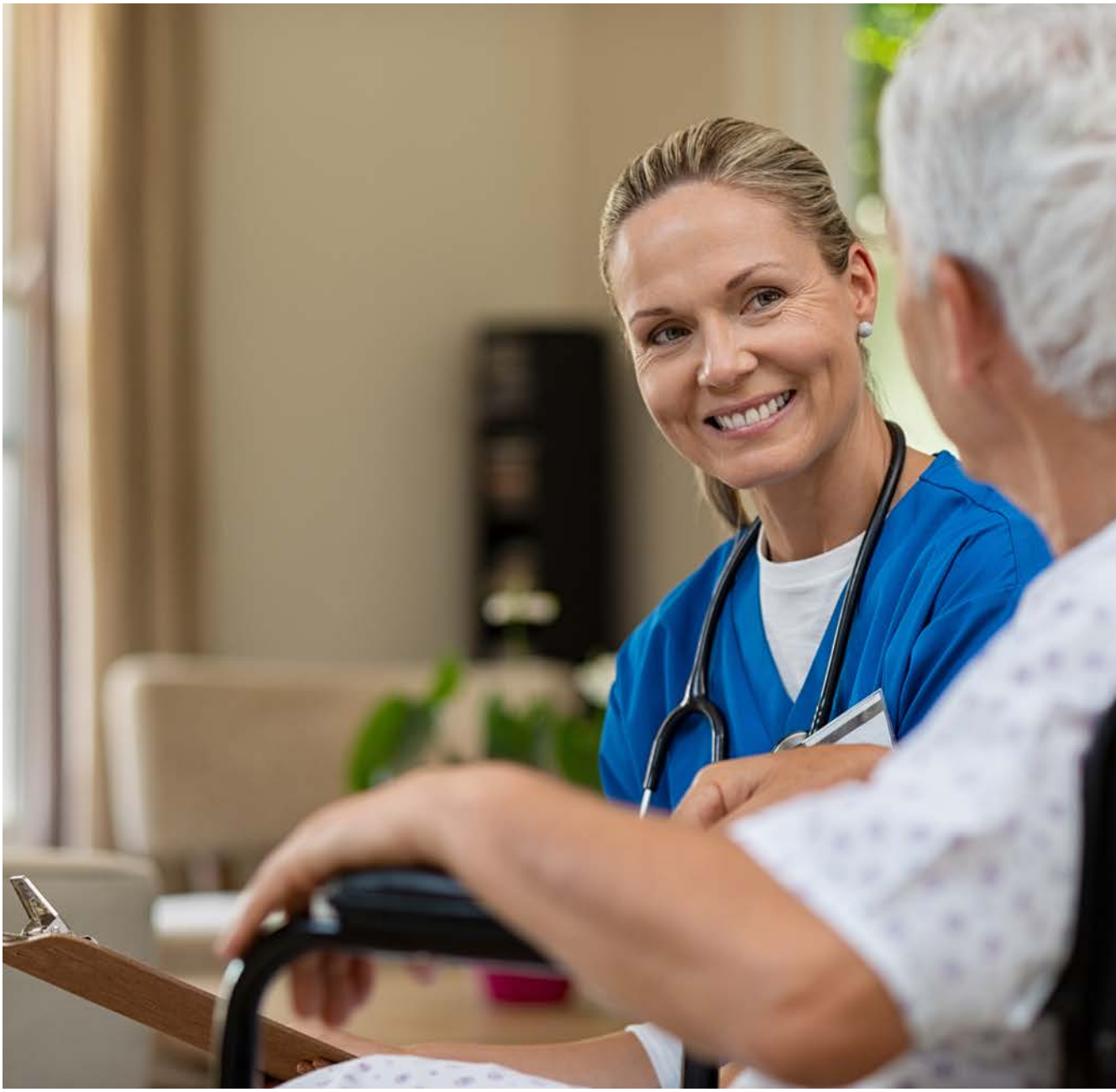
HOME HEALTH CARE: HIPAA & CYBER RISKS

NOV 2019

Brought to you by Health Tech Access Alliance

HIPAA & IT RISKS FOR HOME HEALTH CARE PROVIDERS.



Home health care poses different risks and challenges to protecting PHI, maintaining privacy, and reducing risks from cyber attacks and other threats to security.

HOME HEALTH CARE TODAY

HEALTH TECH ACCESS ALLIANCE

Rapid growth and unique requirements of home health care poses substantial challenges for addressing rapidly growing cyber security threats and patient privacy risks. Meeting these challenges is especially urgent given this sector's vulnerable consumers.

Home health care is often preferred by patients because they are more comfortable in their home as they recover, rehabilitate, or cope with health conditions and aging. Hospitals, payors and other health care providers also recognize home health care can be more cost effective. As a result, the field is growing exponentially with the demand for care rising as the population grows older. According to PHI (phinational.org), the number of adults over 65 is projected to double between 2016 and 2060, and home care is projected to add 1.1 million jobs, the largest growth in any job sector. The sector faces major staffing shortages and resulting training challenges. These challenges are impacting cybersecurity, security and privacy of Protected Health Information (PHI).

Seniors--who make up over 80% of home health care patients according to the *Home Health Chartbook 2019* prepared by Avalere--are already top targets for fraud and scams, especially those that target them because of their lack of knowledge and experience with technology. Identity theft is a major problem for elderly patients. With at least 55% of home health care patients living below the poverty line according to this same study, these patients can be even more vulnerable to identity theft. What few patients or providers realize is health care records are far more valuable than Social Security numbers or credit card information--up to 10x or even 100x more valuable.

At the same time, cyber attacks--pfishing, malware, ransomware, etc--are rising, up 83% since 2010 according to *Home Health Care News, July 27, 2019*. Home health care organizations are beginning to realize how important it is to their reputation, operations and financial well being to maintain PHI data security and privacy, and be HIPAA compliant.

Written by Freya Jimenez. **Photo by** Calvin Stiller.

TRAINING & TECH GAPS: A RECIPE FOR BREACHES

Having staff who are mobile and work remotely, as well as high turnover, poses unique challenges for home health care organizations. Staff typically lack training and use mobile phones, tablets and laptops, which pose significant risks and vulnerabilities to cyber threats.

Proper training for home health care providers regarding privacy and security of data is typically lacking. Often training is only done during orientation and is cursory at best. Training is often conducted by a HR representative or business owner with little HIPAA and data security knowledge or experience. This lack of training, combined with constant turnover of staff--estimated at 40% to 82% by PHI (phinational.org)--along with ongoing staff shortages, is a recipe for data breaches and unauthorized disclosures. Staff also work remotely which means they have Protected Health Information (PHI) on their laptops, tablets or personal devices, and they may travel extensively, sometimes for days at a time in rural areas, before returning to the office. If they do not properly secure their devices or have the necessary device security software in place then they may put their patients data and potentially lives at risk.

Written by Jessica Park. **Photos by** Lee Min-Han.

HEALTH TECH ACCESS ALLIANCE

KEY CHALLENGES & RISKS

1 PATIENT AWARENESS OF RISKS

The elderly are unaware of the medical technology and the importance of PHI themselves

2 STAFF LACK TRAINING

Many home health care staff have little or no experience or training on handling PHI or cybersecurity risks

3 SMALL IS VULNERABLE

Many small health organizations don't understand the requirements of HIPAA HITECH & how to implement needed safeguards, or realize that small organizations are top targets for cyber criminals

4 MOBILE DEVICES & PHONES

Maintaining control of mobile devices & securing mobile communications is challenging

5 FAMILY & PHI

Ensuring PHI is only shared with family if the patient provides permission can be especially difficult in home environments

6 HIGH STAFF TURNOVER

Home health care is growing rapidly, but wages are low and turnover is high, so maintaining trained staff is difficult

7 REMOTE WORKERS

Home health care staff work remotely so monitoring & supervision can be more difficult

8 COST OF TECH & SECURITY

Many home health care agencies can't afford to invest in needed but often expensive technology, training & cybersecurity protection

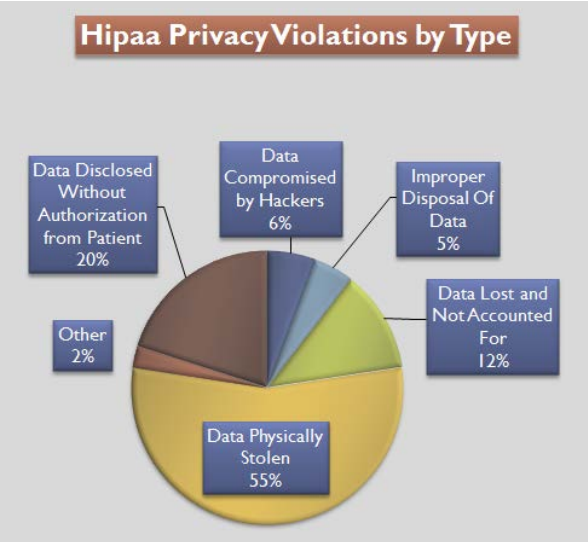
TRAINING & TECH: WHAT WORKS

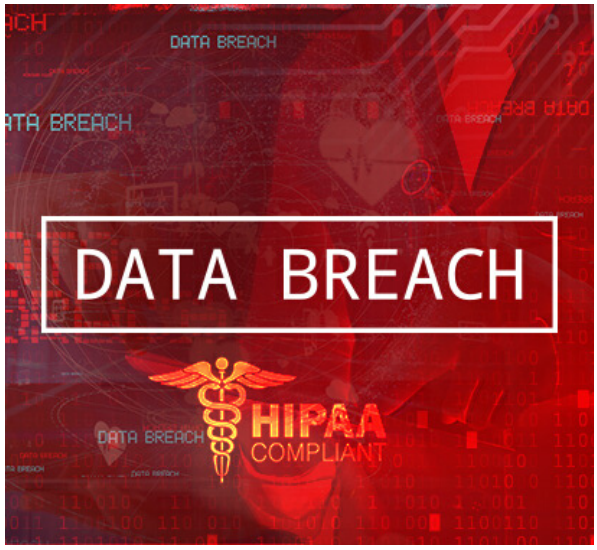
Given staffing and technology challenges, training must be "short & sweet" and technology made simple and affordable to offer real world solutions.

Home health care organizations are starting to look for help in training home healthcare workers and addressing cyber security threats. Training for home health care staff needs to be simple, straightforward and available anywhere for workers to access on demand. Instead of generic HIPAA training, trainings for home health care staff should be short yet comprehensive, practical and relevant to everyday scenarios staff encounter in the field.

While most home health care organizations contract for IT services, Security Risk Assessments should be conducted by an independent, experienced SRA provider to ensure management gains an objective, unbiased and realistic understanding of real world threats, risks, and remediation opportunities. As the demand for home health care continues to grow, finding effective, efficient, and cost effective ways to boost security and compliance will be key for both home health care businesses and for patients.

HTAA offers "short and sweet" 2-3 minute training videos on demand tailored for home health care staff, as well a Security Risk Assessment solutions tailored for home health care organizations. Visit our website www.htaalliance.org for more information.





Written by Jessica Park. **Photos by** Lee Min-Han.

TOP 5 HIPAA MISTAKES IN HOME HEALTH CARE

HEALTH TECH ACCESS ALLIANCE

1 **IMPROPERLY DISCLOSING PHI**

It's easy to have a slip of the tongue and accidentally reveal a patients's private information in conversation. Home health care employees must be mindful of who they are discussing a patient's PHI with. They should only be discussing it with the patient or other authorized individuals.

2 **USING UNENCRYPTED NETWORKS TO STORE OR TRANSMIT PHI**

Home health care staff must be careful to only submit PHI through safe and known encrypted networks. Staff need to have access to a remote encrypted network to store PHI and they must follow the proper HIPAA guidelines regarding transmission of data.

3 **FAILURE TO SECURE PHYSICAL PHI**

Home health care staff are responsible for managing and storing necessary physical devices and hard copy patient data. This can range from managing devices to keeping passwords safe and securing papers that contain PHI. Any papers or electronic devices containing PHI should be stored in secure locations. Physical records must be shredded by authorized personnel or compliant third party service to be disposed of,

4 **ACCESSING PHI ON PERSONAL DEVICES**

Home health care staff should refrain from doing work on personal devices that lack proper password protections, lack encryption or use unsecured networks. This can put patient information at risk by exposing PHI to cyber attacks on vulnerable devices or allowing others access to PHI.

5 **ILLEGALLY ACCESSING PATIENT INFORMATION**

PHI should never be accessed by anyone without the proper authorization. Home health care staff should not discuss clients that they are responsible for with others, even other staff, unless authorized.