ASC 842 Leases and Cybersecurity Risks in Senior Living

Andrea Colfer | Lindsay Francis

BerryDunn

January 25, 2023

Chat Prompt

- Who in the audience has already implemented ASC 842?

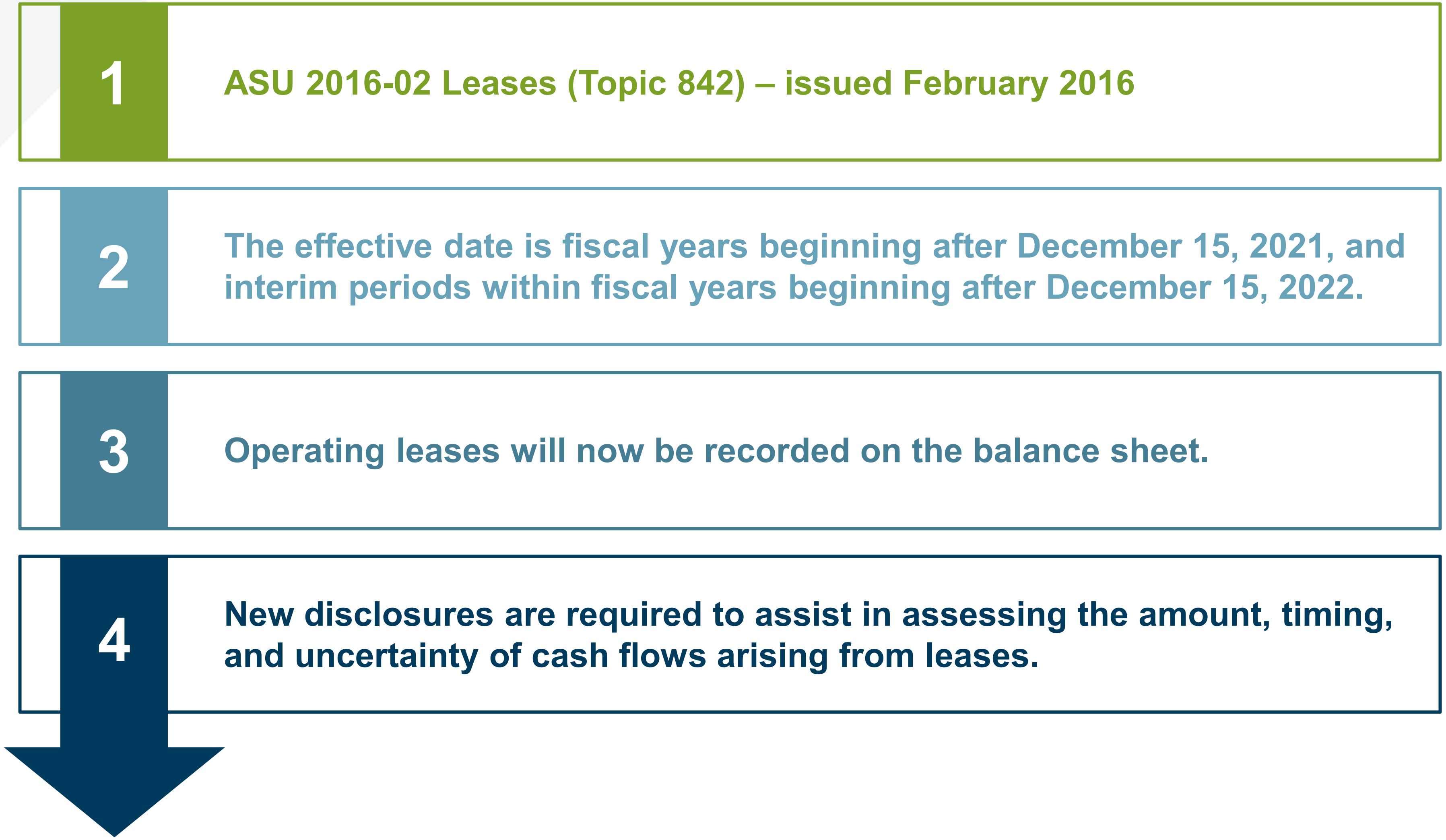
Learning objectives

- Understand the accounting and impact on your financials relating to ASC 842
- Understand the risks that may be present in senior living to both residents and your organization.
- Learn how you can help address the cybersecurity risks prevalent in your organization.

Accounting Standards Codification (ASC) 842 – Leases

Leases

Overview



1 ASU 2016-02 Leases (Topic 842) – issued February 2016

2 The effective date is fiscal years beginning after December 15, 2021, and interim periods within fiscal years beginning after December 15, 2022.

3 Operating leases will now be recorded on the balance sheet.

4 New disclosures are required to assist in assessing the amount, timing, and uncertainty of cash flows arising from leases.

Leases

What is Changing?

1 Capital Leases

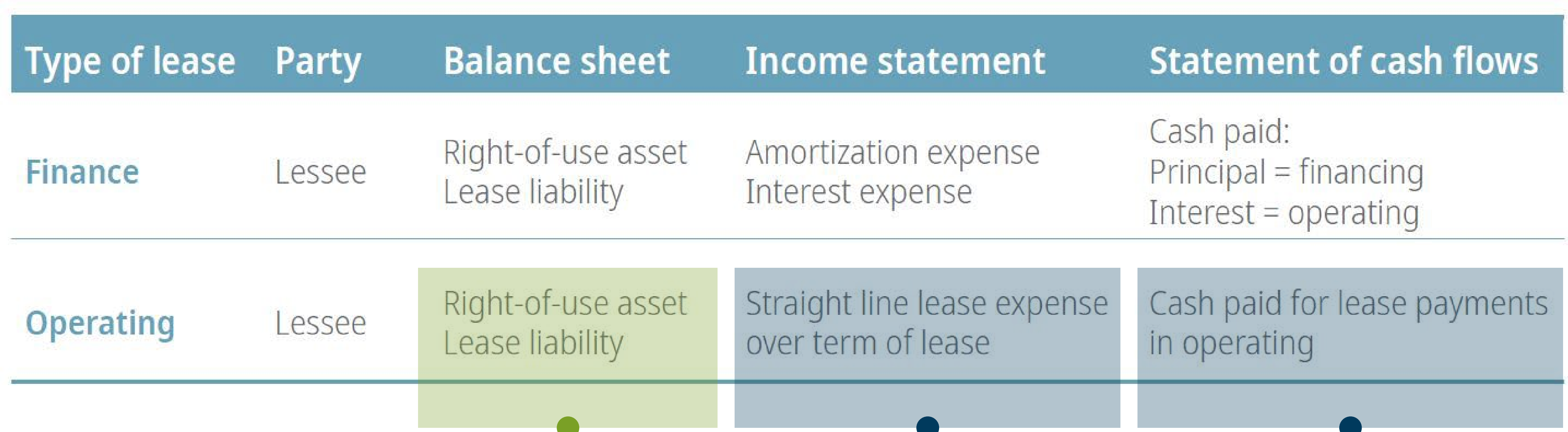
- Will now be referred to as finance leases

2 Operating Leases

- Historically, these have been off-balance sheet commitments requiring financial statement disclosure when material.
- Now will be recorded on the balance sheet via a right-of-use (ROU) asset and lease liability.
- ROU asset and lease liability will be recorded at the present value of payments expected to be made during the lease term.

Finance vs. Operating Leases

https://advisors.berrydunn.com/lease-accounting-guide



Type of lease	Party	Balance sheet	Income statement	Statement of cash flows

Finance	Lessee	Right-of-use asset
		Lease liability
			Amortization expense
			Interest expense
				Cash paid:
				Principal = financing
				Interest = operating

Operating	Lessee	Right-of-use asset Lease liability	Straight line lease expense over term of lease	Cash paid for lease payments in operating

Biggest change

No change

No change

Leases

Balance Sheet and Ratios

	Before ASU 2016-02	After ASU 2016-02
Assets		
Cash	$ 1,000,000	$ 1,000,000
Right-of-use asset	-	250,000
Total assets	1,000,000	1,250,000
Liabilities		
Lease liability	-	250,000
Notes payable	500,000	750,000
Total liabilities	500,000	500,000
Equity	500,000	500,000
EBITDA	**$ 100,000**	**$ 100,000**
DSCR	**1.67**	**0.91**
Debt to Net Worth Ratio	**1.00**	**1.50**

Leases

Other Considerations

1. Discount Rate
2. Transition Methods
3. Disclosures

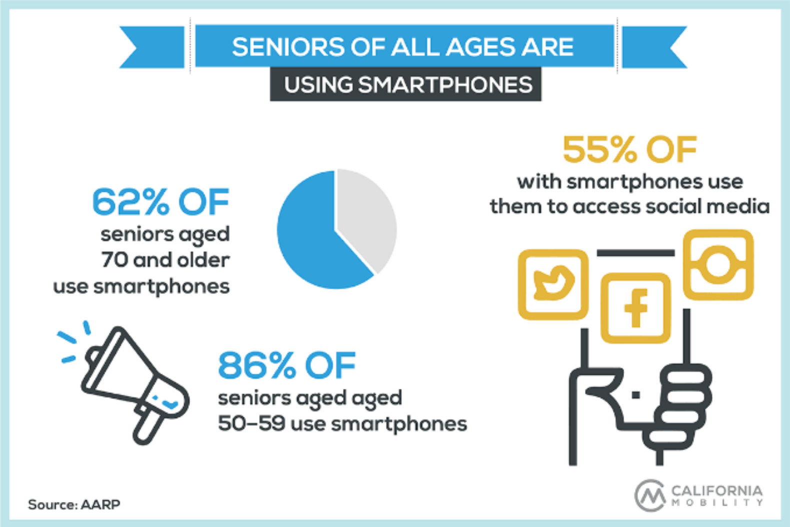
Leases

Key Takeaways

- Effective for reporting periods beginning after December 31, 2021.
- Evaluate if debt covenants need to be modified due to implementation of this standard.
- Establish policies and procedures for lease accounting, including a materiality threshold for assessing leases.

Cyber security

Seniors – Personal Use of Technology … “Silver Surfers”



SENIORS OF ALL AGES ARE USING SMARTPHONES

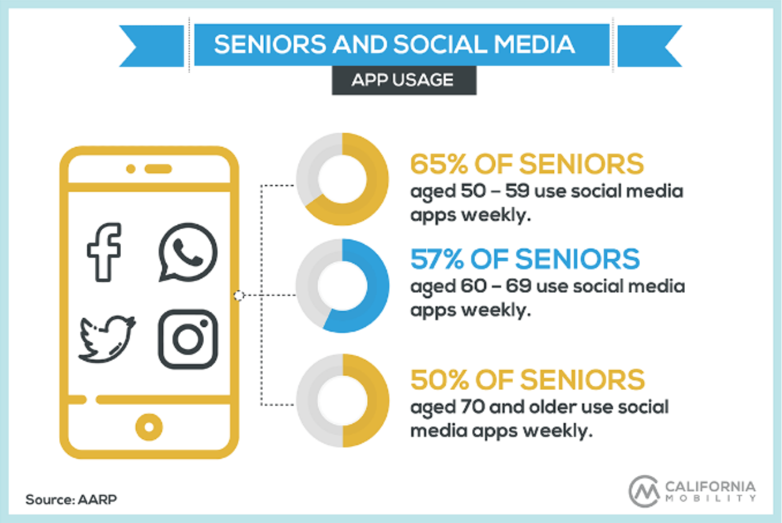
62% OF seniors aged 70 and older use smartphones

55% OF with smartphones use them to access social media

86% OF seniors aged aged 50–59 use smartphones

Source: AARP

CALIFORNIA MOBILITY



SENIORS AND SOCIAL MEDIA APP USAGE

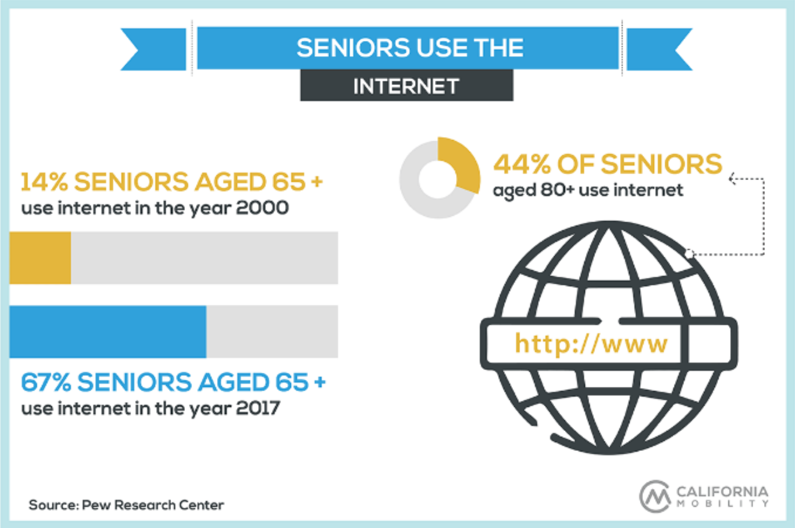
65% OF SENIORS aged 50 – 59 use social media apps weekly.

57% OF SENIORS aged 60 – 69 use social media apps weekly.

50% OF SENIORS aged 70 and older use social media apps weekly.

Source: AARP

CALIFORNIA MOBILITY



SENIORS USE THE INTERNET

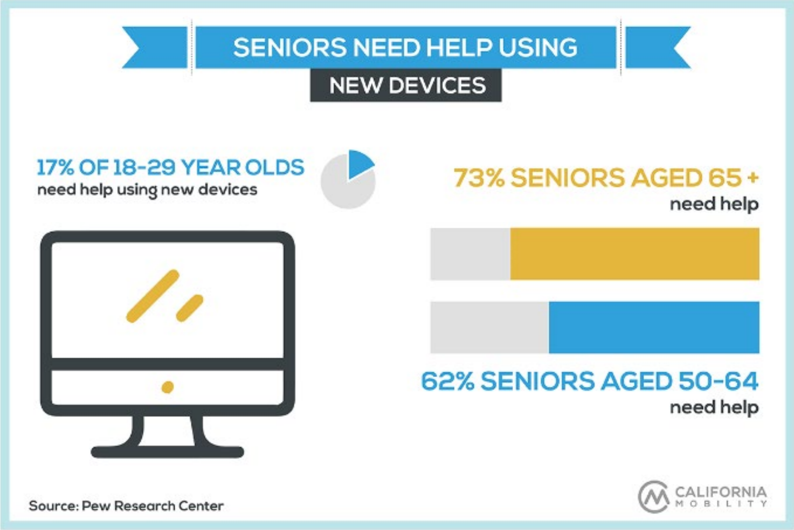
14% SENIORS AGED 65 + use internet in the year 2000

67% SENIORS AGED 65 + use internet in the year 2017

44% OF SENIORS aged 80+ use internet

Source: Pew Research Center

CALIFORNIA MOBILITY



SENIORS NEED HELP USING NEW DEVICES

17% OF 18-29 YEAR OLDS need help using new devices

73% SENIORS AGED 65 + need help

62% SENIORS AGED 50-64 need help

Source: Pew Research Center

CALIFORNIA MOBILITY

Nursing/Rehabilitation Homes Use of Technology

01 Automated IV pumps

02 Portable monitors

03 Smart beds

04 Wearable devices

05 Centralized and mobile patient care computers

06 Electronic health records

07 Telehealth and apps

07 Wi-fi

Senior Living Use of Technology (Assisted and Independent Living)

1. High demand for internet and wi-fi
2. Resident communication systems
3. Grocery delivery, Uber, streaming services
4. Tablet/smart phone use
5. Centralized and mobile patient care computers (assisted living)
6. Electronic health records

Chat Prompt

- What are some unique ways your organization and/or your residents are using technology today?

Where the Risk Lies…

1 Senior scams – via smart phones, emails, and hacking

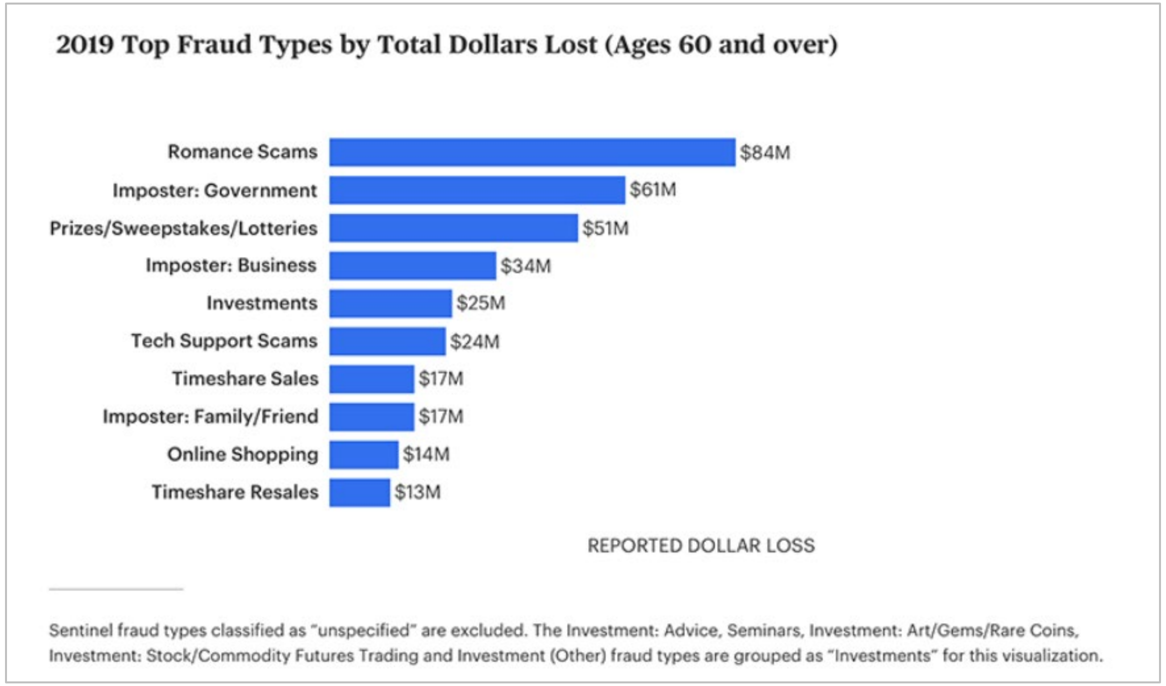
2 Securing networks and devices, but making them accessible for residents and guests

3 Protecting patient/resident data

Risk #1 - Senior Scams

- 2021 – 92,371 reported victims of fraud that resulted in $1.7 billion in losses
- It is estimated only 15-20% of such incidents are reported – why? Embarrassment
- The actual number is estimated to be 3.5 million seniors victims a year with total losses nearing $3 billion

FCC Data – 2019



2019 Top Fraud Types by Total Dollars Lost (Ages 60 and over)

Sentinel fraud types classified as "unspecified" are excluded. The Investment: Advice, Seminars, Investment: Art/Gems/Rare Coins, Investment: Stock/Commodity Futures Trading and Investment (Other) fraud types are grouped as "Investments" for this visualization.

What are Seniors Falling for?

- Imposter scams
  - Family imposter
  - Government imposter
- Romance scams – people ages 70+ had highest median loss from this type of fraud – $9,475
- Sweepstakes scams
- Computer tech scams – this one is rapidly increasing
- Seniors are also unaware of risks related to email – frauds, phishing scams, malicious attachments. This could expose your network to many risks

How to Mitigate The Risk

- Educate your residents
  - Leverage community groups like Centers for Aging
  - Consider having a staff member who is familiar with technology available to help resident – Resident Coordinators
  - Watch out for red flags…..trips to banks, purchases of gift cards, etc.
- Segregate networks – resident/guest networks should be separate and secured
- Have strong firewalls and intrusion detection and prevention tools in place
- You have an obligation to take some measures to protect and educate your residents

Risk #2 - Securing Networks and Devices

- With mobile computer, tablets, laptops – wi-fi is not a luxury, but a requirement
- Residents and guests also require reliable internet
- If unsecured, may be a gateway into your business and applications
- Risk of ransomware
- Assisted/independent living – if residents have own routers and internet – make sure they are securing their network

How to Mitigate The Risk

- The network should require a complex password to connect, and it should be changed on a periodic basis.
- Segregate networks – resident/guest networks should be separate and secured. The business network should not be broadcast as findable.
- Have policies on the use of wi-fi. Require staff to be on business network when doing business. Do not allow personal devices to connect.
- Have strong firewalls and intrusion detection and prevention tools in place.
- Consider the use of a third-party to help offer and manage solutions.

Risk #3 - Securing Patient/Resident Health and Other Data

- Personal health data that must be protected under HIPAA laws is present.
- Aides, nurses, and others may use personal devices – such as phones to text over patient care.
- Health data is being transmitted over wireless networks. Are those secured?
- Mobile and wearable technology that monitors and tracks patient health – how is that secured?
- Assisted/independent living may also have to be aware of credit card information – how is that protected?
- Physical security of facilities.

Chat Prompt

- How often is your organizing reviewing operations for compliance to HIPAA?

How to Mitigate the Risk

- Consider doing a check-up on your compliance with HIPAA rules
- Only allow authorized devices to be used for patient care and information
- Encryption – of laptops, of phones, and of data in transit
- Train employees on HIPAA privacy and rules
- Understand how third-parties you may use for managing networks/IT are addressing HIPAA requirements
- Secure how IT equipment is secured and tracked
- Secure paper files and destroy paperwork properly

18% of healthcare workers in a recent survey done by Kaspersky said that they did not know what HIPAA was

Only **one third of healthcare workers** said they were aware of their organization’s cybersecurity policy

Cyberattack Preparation

Training—phishing attacks

- Phishing is the most common way hackers get ransomware and malware installed
- It only takes one click
- Frequent training is key – questioning emails becomes habit/culture
- You are not hurting feelings by testing
- Other controls should also be in place
- Prevent users from being able to install software (local administrator rights)
- Allow and deny list for software
- Disable macros in email

59% of nonprofits do not provide any cybersecurity training to staff on a regular basis

Final Thoughts

- Training and education is just as important for your residents as it is for your employees
- Leverage third-party support and expertise where you are able – this includes many not-for-profit organizations who offer resident education programs
- Your organization is responsible for protecting health and personal data and will be held accountable in the event of a breach
- And, as always…stop clicking without thinking!