



# Community and Advisory Board Meetings

Spring 2021

# Agenda

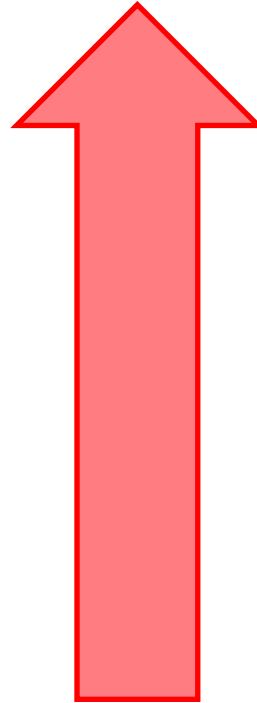
1. Curi Updates
2. Health Policy News
3. Cybersecurity Update
4. COVID-19 Civil Immunity (& Other Liability Updates)

# 2020 Peer Comparison—Curi

	2020	Rank	Industry Avg
Assets	\$756 million	#14	\$581 million
Surplus	\$333 million	#14	\$288 million
Gross Written Premium	\$140 million	#12	\$79 million
Net Written Premium	\$91 million	#13	\$61 million
Growth in Assets	14.3%	#3	3.9%
Growth in Surplus	-0.6%	#25	2.2%
Growth in GWP	-2.6%	#15	1.8%
Growth in NWP	1.0%	#12	-3.6%
Calendar Year Loss Ratio	86.7%	#22	84.9%
Expense Ratio	21.0%	#11	27.9%
Combined Ratio	107.7%	#16	116.9%

# MPL Market Trends

- » Combined ratio
- » Number of Suits
- » Severity
- » Indemnity
- » Defense Costs
- » Reinsurance cost
- » MPL Premiums



YOUR COMPANY

# We're here to serve you. Always.

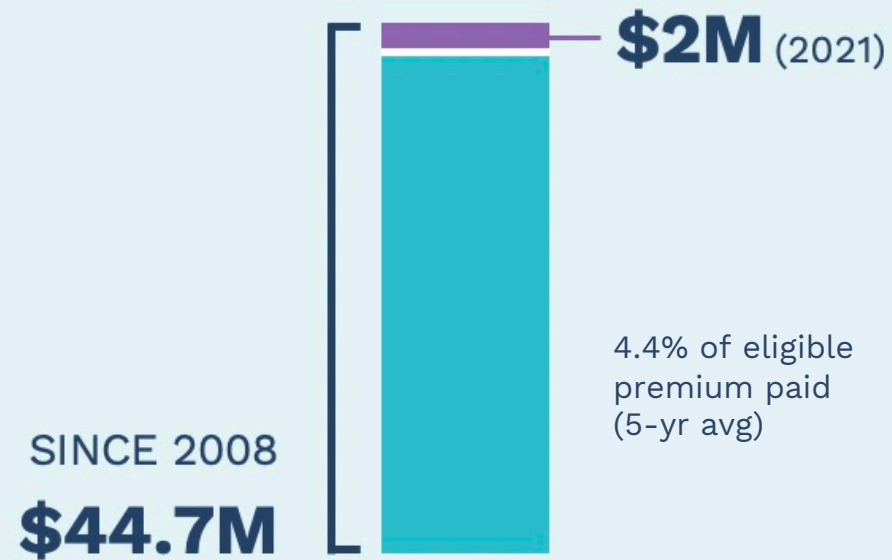


**Our products and services are built to help you and your practice**—from insurance and investments to business services and emotional and physical wellness.

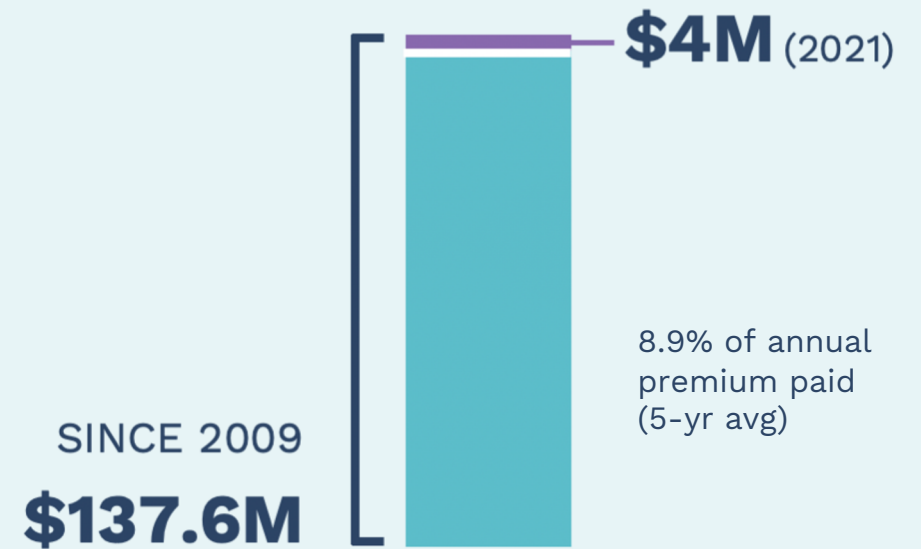
**By staying curious about you**, we're able to build the best solutions to meet your needs—now and well into the future.

# Dividends & Legacy Fund

## Member Dividends



## The Legacy Fund



# We curate business solutions to help you thrive and prosper.

**Every year, operating a medical practice seems to get more challenging.** Your main focus is your patients. Curi's main focus is you. With more than four decades of physician input, we know what it takes to keep your practice running strong. You tell us your problem—we'll source the best solutions.

## Curi Advisory Specialties:

- Strategic guidance
- Operational expertise
- Financial analysis
- Payor contract negotiations
- Data and analytics
- Reputation management

# Curi Advisory Questions

1. What three management tasks take the most of your time?
2. If you outsource any management or operational services, which of these are you still not satisfied that they are bringing maximum value?
3. Would you consider using an outside advisory firm to minimize operational expenses or improve revenue?
4. What unmet needs do you have today for which you cannot find help because either cost effective, or accessible solutions don't currently exist?



# COVID-19 Deferred Premium (CDP)


- » Suspended all premium invoicing & automatic bank drafts from March 23, 2020 – June 30, 2020.
- » All delayed premiums were combined into a separate balance known as CDP.
- » CDP balance were billed over a 12-month period beginning July 1, 2020 through June 30, 2021.
- » CDP must be paid by check or through our portal:  
<https://fcb.billeriq.com/ebpp/curi/>

# Agenda

1. Curi Updates
2. Health Policy News
3. Cybersecurity Update
4. COVID-19 Civil Immunity (& Other Liability Updates)

# Interoperability & “Information Blocking” Rule

- » Implements 21<sup>st</sup> Century CURES Act requirements
- » New effective date: April 5
- » Basic rule: Electronic Health Information must be made readily available in a timely manner at no cost to patients and their representatives (& reasonable cost to other permitted recipients)
- » Penalties for engaging in activities considered “information blocking,” unless an exception applies (8 exceptions)
- » Curi resource: [www.curi.com/cures-act](http://www.curi.com/cures-act)



In March 2020, the Office of the National Coordinator (ONC) for Health Information Technology released the interoperability and “information-blocking” rule as a part of the 21st Century Cures Act (Cures Act). It seeks to increase health data exchange and limit refusals to share health data. Read more on the Cures Act using the following link: [Final Rule](#).

The rule includes a provision requiring that patients be permitted to electronically access all of their electronic health information (EHI). Access must be granted whether the data is in a structured (chosen from a list or a drop-down menu) and/or an unstructured (free text) format, unless one of eight exceptions to the Final Rule applies. EHI generally must be made readily available **at no cost to patients and their representatives**, and at a reasonable cost to others permitted to receive the EHI. **This new rule goes into effect on April 5, 2021.**

The information-blocking part of the Final Rule applies to these three categories of organizations, called “actors” in the Final Rule:

- healthcare providers;
- health IT developers of certified health IT, and;
- health information networks, or health information exchanges.

# Telehealth—A Pathway Forward

## Short Term

- » Waiver of many Medicare requirements
- » Able to bill for more services
- » 2021 Physician Fee Schedule codified some changes

## Medium Term

- » MedPAC: extend provisions & study for limited time (one or two years)
- » Substitution or add-on?

## Long Term

- » Congressional action to expand telehealth
- » Telehealth parity legislation?
  - State action likely before federal action

# Ongoing Federal Financial Support

## » Temporary suspension of sequestration cuts

- 2% Medicare FFS increase
- Expires March 31, 2021, unless extended

## » \$3 billion added to Medicare Physician Fee Schedule

- Will prevent cuts to certain specialties

## » Provider Relief Fund reporting requirements

- Portal open for registration
- Deadlines not yet established
- <https://www.hhs.gov/coronavirus/cares-act-provider-relief-fund/reporting-auditing/index.html>

# Agenda

1. Curi Updates
2. Health Policy News
3. Cybersecurity Update
4. COVID-19 Civil Immunity (& Other Liability Updates)

# National Cyber Security Alliance Guidance

- » First call to action: Do not allow continued use of **Windows 7** (83% of imaging devices run on outdated operating systems like Windows 7); get rid of old legacy systems
- » Second call to action: People need to be trained in technology, to be sure that they understand what to do to avoid being hacked and what to do during a potential hack
- » Third call to action: Make sure whatever third-party vendors you're dealing with have just as robust a security policy as you have for yourself
  - Robust passwords
  - Multi-factor authentication
  - **Current Curi approved BAAs with all vendors who touch PHI**

# Cybersecurity Resource Guide

- » How to Avoid Becoming a Victim
- » Phishing Quiz
- » If You Are Attacked
- » Lessons Learned from a Cyber Event
- » Steps During a Crisis
- » Post-Crisis Steps
- » Checklist for the First 24 Hours Following a Breach



## Cybersecurity: A Risk Management Resource Guide

Data security is an essential part of business in today's highly technical world. Training all employees, including medical providers, associates, and information technology (IT) technicians, is an integral defense strategy and may prevent your practice from falling victim to a data security breach.

According to Experian's *Managing Insider Risk through Training and Culture Report*, 66% of data protection and privacy training professionals surveyed labeled their employees the "weakest link" in safeguarding their organization from cyber threats.

In CompTIA's *International Trends in Cybersecurity* research, 52% of survey respondents felt cybersecurity issues were caused by human factors. In fact, most cybersecurity breaches are a direct result of users lured by nondescript links and payloads delivered via browsers and email, respectively.

### HOW TO AVOID BECOMING A VICTIM

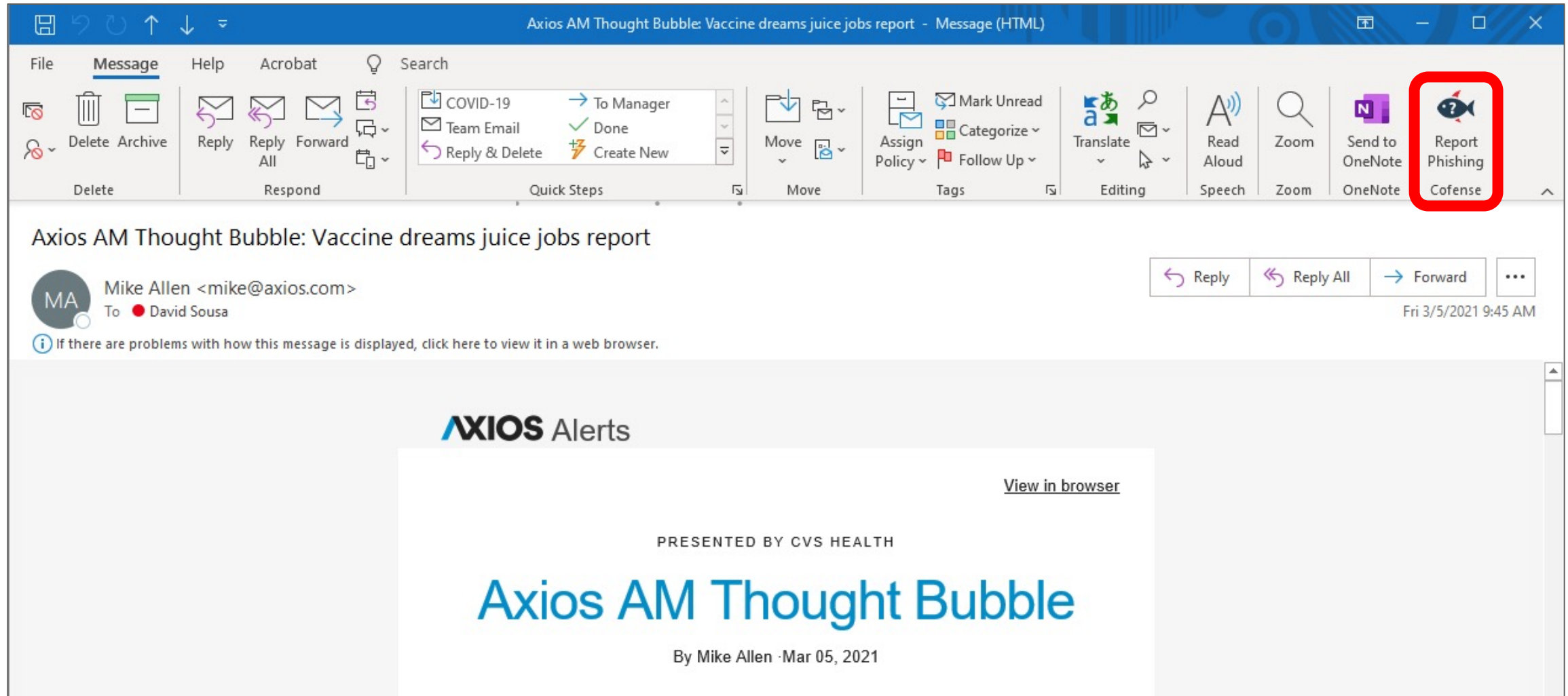
Here are some best practices to follow from leading industry experts:

- Educate your employees. Security awareness training is more than just HIPAA training. It is essential to teach employees to look for warning signs of security threats and how to avoid them (for instance, not downloading files from suspicious emails). If anything looks suspicious, have your IT department check it before clicking. Conduct **mandatory** annual privacy and security training. In-person training is recommended, as this ensures everybody is actively participating. Sometimes, online training can be ineffective as employees may run the training in the background while doing other work.
  - Employees must understand the importance of ensuring confidentiality of patient information. Employees should know not to share any patient-protected health information, commonly known as PHI and understand what those PHI identifiers include.
  - Retain evidence of all employee training and related emails for at least six years. If an Office of Civil Rights (OCR) audit or investigation were to occur, you might be asked to prove your practice is keeping up with workforce education. This recommendation is based on trends seen with the OCR.
- Ask your IT staff to configure web filtering to update frequently and block information being sent outside of the firewall to suspicious IP addresses. Also, have an IT security vendor conduct penetration (pen) testing. In pen testing, a hired outside IT security professional attempts to penetrate your systems.

800-662-7917 | [www.curi.com](http://www.curi.com)



# One Source/Cofense Resources





The screenshot shows the Outlook interface for an email titled "Axios AM Thought Bubble: Vaccine dreams juice jobs report". The ribbon is set to "Message". A red box highlights the "Report Phishing" button in the "Cofense" group on the ribbon. The email content includes a header from Mike Allen to David Sousa, a link to view the message in a web browser, and a main body with the "AXIOS Alerts" logo, a "View in browser" link, and the text "PRESENTED BY CVS HEALTH Axios AM Thought Bubble By Mike Allen · Mar 05, 2021".

# Available Now



## Managed Security Store

### Managed Security Products

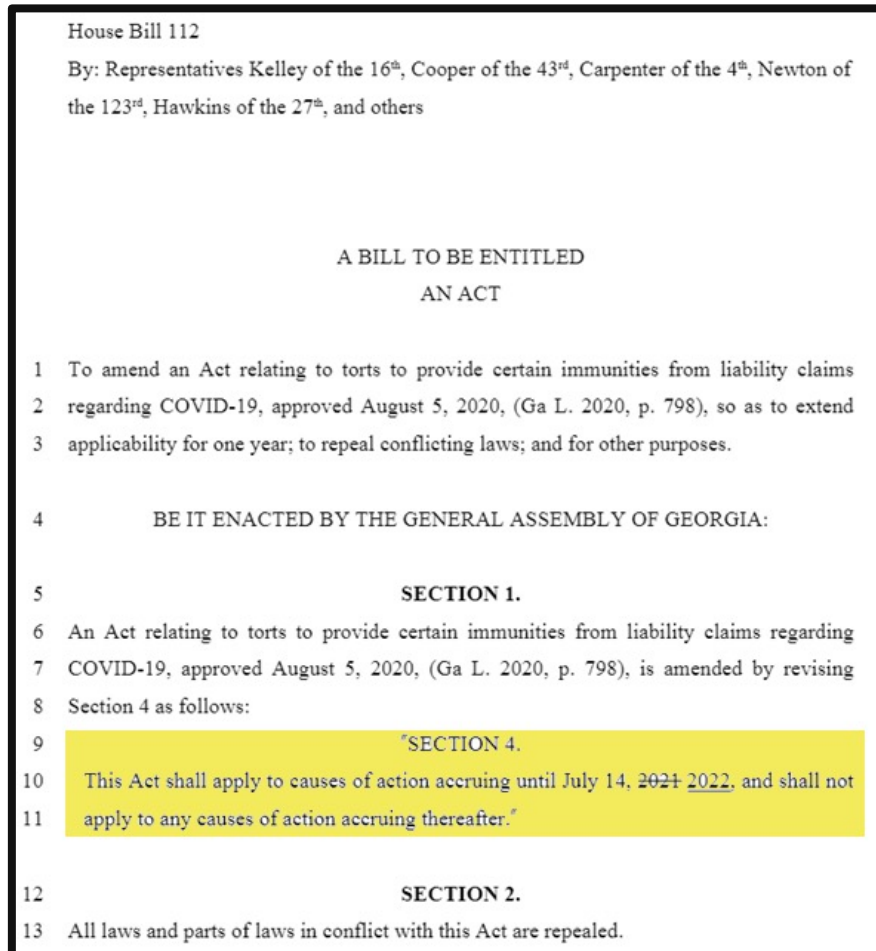
 <p><b>Internal + External Threat Assessment</b></p> <p>Conduct an assessment of both external risk exposure and internal cybersecurity infrastructure / defense systems</p> <p><a href="#">Learn More</a></p> <p><b>ORDER</b></p>	 <p><b>Internal Threat Assessment</b></p> <p>Evaluate the health of your cybersecurity infrastructure and defense systems from the inside out</p> <p><a href="#">Learn More</a></p> <p><b>ORDER</b></p>	 <p><b>External Threat Assessment</b></p> <p>Quickly assess your cybersecurity vulnerabilities and environmental risks</p> <p><a href="#">Learn More</a></p> <p><b>ORDER</b></p>	 <p><b>Cofense PhishMe™</b></p> <p>Improve employee response to phishing attacks and empower employees to provide real-time threat intelligence</p> <p><a href="#">Learn More</a></p> <p><b>ORDER</b></p>	 <p><b>Cofense Triage™</b></p> <p>Orchestrate entire phishing incident response process to reduce noise and stop threats in real-time</p> <p><a href="#">Learn More</a></p> <p><b>ORDER</b></p>	 <p><b>Cofense PhishMe™ + Triage™</b></p> <p>Leverage real-time threat intelligence from employees to efficiently block security threats as they arise</p> <p><a href="#">Learn More</a></p> <p><b>ORDER</b></p>
---	--	---	--	--	---

# Agenda

1. Curi Updates
2. Health Policy News
3. Cybersecurity Update
4. COVID-19 Civil Immunity (& Other Liability Updates)

# GA—COVID Civil Immunities Extended

» HB 112 introduced to extend civil immunities until July 14, 2022:



» Our thanks to:



- » Recall that the immunity, per SB 359, is limited to claims for:
- **“Transmission, infection, exposure or potential exposure to COVID-19” claims (PI and death)**
  - **Treatment related to COVID-19**
  - **PPE**

# Status of COVID-19 Civil Immunity

In Our 5 Core States:



» Blanket civil immunity for all care rendered in declared state of pandemic emergency:

- Granted by Exec Orders in **NJ** and **VA**
- Granted by Legislation in **NC**

» Limited civil immunity by Exec Order in **GA**

» No immunity at all in **PA**

\*Some form of immunity in 20 other states (as of 11/2020): AL, AR, AZ, CA, CT, HI, IL, IN, KS, LA, MA, MD, MI, MS, NV, NY, OK, UT, VT, WI

# A National Reach (*Impact on our Tort Systems*)

- » Thirty-three states and the District of Columbia (as of 3/1/2021) have enacted protections from COVID liability claims either through legislation or executive orders
  - But no changes over the five-month period (11/20–3/21) in our core states.
  - FLA added sweeping reform 3/24/21
  - NY stripped nursing homes on 3/24/2021 of immunities previously granted