***WPMT-TV*, York**
Blue Ridge fiddles heartstrings with Touch A Heart campaign for Valentine's Day

Fierce Video
Comcast should sell its Hulu stake to Disney in 2021: analyst

Next TV
Facebook Board Reviewing Donald Trump Ban

LightReading
Why Verizon keeps promoting 5G at the Super Bowl

Poynter
***Philadelphia Inquirer* kills comments section on most stories**

Associated Press
Snow delays Pa. governor's budget address a day

Philadelphia Inquirer
Pennsylvania got through the 2020 election. Now for the hard work of building a new election system.

Pittsburgh Tribune-Review
Editorial: Dermody's upward fall is all-too-familiar in political world

Hackers are increasing their attempts to break into health-care companies, putting additional pressure on an industry already struggling with managing the coronavirus pandemic.

Persistent threats come from ransomware gangs, financial scammers and hackers backed by nation-states, current and former hospital security chiefs say. "The logs and the graphs show, oh, man, these have ramped up, it's hard to deny that," said Christopher Stroud, technology manager at Great Plains Health, a hospital based in North Platte, Neb., that serves around 183,000 patients a month.

Great Plains Health normally blocks around 10,000 attempts to access its servers daily, Mr. Stroud said. After it began its first coronavirus antibody drug trials in November, it saw that number triple on average, he said. Some days, attempts have reached 70,000. Intelligence agencies in the U.S., Canada and Europe have warned repeatedly that nation-state-backed hackers and cybercriminals are attempting to break into health-care systems to steal vaccine-related research and other data. A former cybersecurity specialist in the U.S. Navy, Mr. Stroud sees the hallmarks of nation-state actors in some of the attacks against his hospital.

The hacking blitz comes as the health-care industry reported a bruising year of data breaches in 2020, particularly as the effects of the pandemic began to set in. Security and technology staff at hospitals suddenly had to deal with an expanded remote workforce, Covid-19 patients swamping wards and the setting up of makeshift sites for virus testing. "It was a terrible second half of the year. It's been some rough, rough going for health-care organizations," said Drex DeFord, a health-care consultant for Critical Informatics Inc., a cybersecurity firm also known as CI Security. He also previously served as a chief information officer at San Diego's Scripps Health and at the Seattle Children's Healthcare System.

Data reported to the U.S. Department of Health and Human Services shows that almost every month last year more than 1 million people were affected by data breaches at health-care organizations. Under the Health Insurance Portability and Accountability Act, organizations that handle patient data must report breaches involving 500 people or more to HHS within 60 days. Hospitals and clinics cite a variety of reasons for the breaches, including improper records disposal, device theft and natural disasters. Hacking or compromised technology, however, are the primary culprits.

As the coronavirus pandemic spread last spring, health-care providers were placed in a difficult position. Adding to the need to care for large numbers of Covid-19 patients, hospitals experienced a revenue crunch through the canceling of elective procedures because of the virus and the reallocation of resources to response efforts. The American Hospital Association estimates that between March and June, this resulted in more than $200 billion in Covid-19-related expenses and lost revenue, before accounting for government financial relief.

Hospitals were unable, or unwilling, to finance significant security projects at precisely the time they needed to, said Jared Phipps, senior vice president of world-wide sales engineering at cybersecurity vendor Sentinel Labs Inc. Ransomware attacks, which lock up vital systems or data, are a particular scourge as downtime can threaten lives. Prosecutors in Germany, for instance, recently investigated whether a September ransomware attack on a hospital in Düsseldorf contributed to a woman's death, after she had to be diverted to another facility for emergency care because of the incident.

The Justice Department on Jan. 27 said that it had coordinated with international law-enforcement agencies to disrupt a group responsible for ransomware known as NetWalker that had targeted hospitals. Health-care providers often use a patchwork of systems from third parties rather than their own technology, which exposes them to supply-chain risks, said Terry Ray, senior vice president and fellow at cybersecurity firm Imperva Inc.

A ransomware attack early last year at Blackbaud Inc., which provides cloud services to hospitals, schools and other nonprofits, compromised the data of hundreds of customers. In September, medical facilities reported to HHS that nearly 10 million individuals had their information breached. At least 46 have cited the Blackbaud episode in letters to state regulators. “When that happens, unfortunately, the health-care organization winds up on the wall of shame, not the vendor,” said Mr. DeFord of Critical Informatics.

A spokesperson for Blackbaud said the company regrets the incident. “We have already implemented changes to prevent this specific issue from happening again,” the representative said. Some hospitals have tolerated lax security measures for too long, said Austin Berglas, global head of professional services at cybersecurity business BlueVoyant LLC and a former cybersecurity specialist with the Federal Bureau of Investigation.

Health-care organizations often neglect cybersecurity basics, such as using two-factor authentication and running the latest operating systems, he said. He has seen some hospitals leave sensitive information on unprotected servers, as cybersecurity isn’t seen as a priority and doesn’t always receive enough funding. Internet-connected devices at hospitals also bring risks because they sometimes aren’t designed with security in mind, he said. “We’re not even asking the adversary to bring their A-game to break in there,” he said.

For Mr. Stroud of Great Plains Health, the risks aren’t theoretical, but personal. The hospital was the victim of a ransomware attack in November 2019, and while he said it didn’t have to turn patients away and managed to recover quickly, the experience showed him that a lack of investment in cybersecurity in the health-care sector can lead to disaster. “I work for the hospital that I go to, that my parents go to, and that my kids go to. And so you really want best-of-breed [technology] everywhere you go because at the end of the day,” he said, “it could be you in that bed.” – ***Wall Street Journal***

Pennsylvania elections officials have never done this before, and they’re bracing themselves for trouble. As part of the new vote-by-mail system, state law now allows voters to sign up for a “permanent list” to automatically receive mail ballot applications every year. The law says counties have to send those applications by the first Monday in February

It’s been an administrative headache for county elections offices, which in some cases have to send more mail at once than ever before. Montgomery County, for example, sent ballots in batches of tens of thousands at a time last fall. On Monday, it’s sending a massive mailing of letters and applications to 196,000 voters. And elections officials are worried about voter confusion, ranging from those who believed the permanent list meant they would automatically be sent *ballots* — not applications — to voters who don’t remember signing up for the list and aren’t sure why they’re receiving a mailing. “This is a whole brand-new component that nobody has yet experienced,” said Lee Soltysiak, Montgomery County’s chief operating officer and chief clerk of its elections board.

The county has hired temporary workers in preparation for the applications and phone calls officials anticipate will soon begin flooding in. “We’re preparing for a prime-time, high-turnout-election kind of interest over the next couple of weeks because of these letters dropping,” Soltysiak said. The rollout of the permanent list mailings has been bumpy, with counties initially unable to obtain accurate data and then receiving correct data and materials just two weeks before the deadline. Some growing pains are to be expected — especially following a challenging, tiring election just a few months ago — but several officials said that it’s been a frustrating experience and that they’re worried the headache will become an annual migraine. “It’s a nightmare for us, logistically,” said Sara May-Silfee, election director for Monroe County in Northeastern Pennsylvania. She had prepared a booklet to better explain the mailing to

voters but had to scale back her plans because the Pennsylvania Department of State didn't send materials and data until Jan. 15.

In Lycoming County, in northern Pennsylvania, elections director Forrest Lehman said he had originally planned to print and mail the applications and letters in-house, but the state's delay forced him to enlist an outside vendor, costing the county money. Christine Reuther, a Delaware County Council member who works with the elections departments, was reminded about the permanent list when a reporter asked about it last week. "Wow, I hadn't focused on that at all. We need to get those printed. That means we need to get those printed," she said, before asking when the mailings have to be sent. Monday. "Oh, that's not going to happen in Delaware County," Reuther said.

On Sunday, Reuther confirmed the applications wouldn't be mailed out by Monday. Counties like Delaware County that have been dealing with the near-constant demands of lawsuits since the election and associated demands for documents and data are behind in other time-sensitive tasks," she said, calling the permanent list mailing "another unfunded mandate from the state in terms of staff time and printing and mailing costs." A spokesperson for the Department of State said "the first year of any new provision is always the most challenging" and encouraged voters to visit the department's website for more information. Under the law enacted in late 2019, voters can sign up for a permanent mail voter list when they apply for mail ballots. But it's not what it sounds like.

Here's how it works: When voters add themselves to the list, they automatically apply for mail ballots for every election just *that year*. Many who requested mail ballots in last year's primary election, for example, were automatically signed up to receive ballots for the general election in November. Voters are automatically sent ballots only during one calendar year. After that, they'll receive ballot *applications*, which they can once again use to sign up for ballots in all elections that year. (This doesn't apply to voters with disabilities, who have long had a separate permanent list that actually does involve permanently receiving ballots.)

The mailings being sent now are going out to all voters who checked the box for permanent status. Voters have to fill out an entire ballot application again to receive mail ballots. Voters can request to cancel their application and remove themselves from the list. Otherwise, they'll continue receiving an application at the start of every year. Voters can also fill out the application online at votespa.com/applymailballot. The permanent list created a lot of confusion last year, when voters who didn't realize they were on it submitted hundreds of thousands of duplicate applications for mail ballots, overwhelming already overworked elections offices.

A spokesperson for the Department of State didn't have the number of permanent list voters Friday, but there were 1.5 million such voters after last year's primary, and the number has only grown since. Based on numbers provided by several counties, most voters who requested mail ballots last year appear to have also signed up for the permanent list. That means a lot of voters will soon be receiving applications who might not remember checking the box. "I'll be fascinated to see how many people cancel their mail-in applications," said Thad Hall, elections director for Mercer County, in Western Pennsylvania. "A lot of those people are people who I think didn't mean to sign up to be a permanent voter."

Then there are voters who do remember signing up for permanent status, but thought it would mean permanently being signed up to receive ballots — not to have to submit an application every year. "If you're going to have something permanent, why don't you make it permanent?" Hall said. Future years should be less bumpy, county elections officials said, but they saw several challenges that will persist.

It's expensive to print and mail the letters and applications, and for some counties this will be the largest mailing all year. It's also a technical and logistical challenge to make sure all the right materials go to the right people. "A mailing to over a quarter-million people is never a simple task," said Nick Custodio, deputy commissioner for Philadelphia City Commissioner Lisa Deeley, the chief elections officer. The city commissioners are sending applications Monday to all 282,000 voters on the permanent list. "It's definitely yet another unfunded mandate that the counties are having to absorb this February," Custodio said. "Just look at postage alone on 280,000 letters." County elections officials also worry about the list growing to a monstrous size, similar to the way voter rolls are messy and sometimes difficult to maintain. – ***Philadelphia Inquirer***

The pockets of high-speed internet wasteland that pockmark Pennsylvania are shameful in an age when good internet accessibility is as ubiquitous, for most, as postal service and electricity. And in this pandemic moment in time, those deserts of affordable and reliable connectivity threaten quality of life and education, creating two classes of citizens — the haves and have-nots — on opposite sides of a digital divide.

The lack of reasonably priced and dependable internet access — the kind of high-speed access that allows students to connect to their lessons and citizens to connect in a safe way to their family members — should be of top priority for state legislators. It's a problem evident in both rural and urban areas, but especially in rural and semi-rural areas. Within an hour's drive of Pittsburgh, there are communities where residents with spotty or slow internet speeds cannot do a Google search or stream a movie unless they have the means to pay for special equipment/service that still does not provide access equal in cost and dependability to the kind of connectivity taken for granted by most Pennsylvanians. Slow internet speed can mean extended time downloading information and images from the internet. When more students across the state are relying on home computers during COVID-19, this undermines learning.

A recent study by the Joint State Government Commission has acknowledged the pandemic has put regions without broadband access at a disadvantage in health care, education, agriculture and economic development. Expansion of the broadband network has been primarily developer driven, with providers expanding service according to market demands. But, when it comes to this essential service, the infrastructure must be given a push by government. Pennsylvania took a critical first step by enacting two state laws last year: Act 132, which provides $5 million — a pittance — to help start a broadband expansion fund, and Act 98, which eases restrictions on the ability of rural electric cooperatives and cable companies to attach broadband units to existing utility poles. Now the purse strings must be loosened and essential funding for grants and loans must be put in place and in amounts large enough to get the job done.

Those lacking good broadband service is estimated at some 800,000 people. The cost estimate for bringing all of Pennsylvania into the digital age ranges from millions to billions of dollars, depending on who is doing the estimating. In 2019, the Governor's Office of Broadband Initiatives put the figure at between $500 million to $1 billion. Gov. Tom Wolf has proposed a natural gas severance tax to fund the initiative, a proposal that has never gained traction.

Kinber (the acronym for the Keystone Initiative for Network Based Education and Research, a nonprofit based in Harrisburg) and Morgantown, W.Va.-based ClearFiber Communications are demonstrating one way to do it; the partners are planning an 81-mile broadband cable through parts of Washington and Greene counties to serve 2,000 homes. Partnerships are likely to be the gold standard in pushing good internet access to all corners of Pennsylvania. The Pennsylvania Legislature can help with dollars and sense. Eliminating the

state's digital haves and have-nots is an imperative mission of fairness as well as an investment in future productivity. – ***Pittsburgh Post-Gazette*** **editorial**