Congress of the United States

Washington, DC 20515

April 16, 2024

Bruce Siegel, MD
President and CEO
America's Essential Hospitals
401 9th Street, NW, Suite 900
Washington, DC 20004

Dear Dr. Siegel:

We write to request that you urge your member hospitals to protect American patients' medical privacy from abusive legal demands by state attorneys general (AGs). According to a recent Senate Finance Committee Majority Staff Report entitled, "How State Attorneys General Target Transgender Youth and Adults by Weaponizing the Medicaid Program and their Health Oversight Authority" state-level politicians are abusing their legal authority to attack transgender patients for political gain, while undermining faith in the Medicaid program. In at least four states, AGs have abused their legal powers to demand that hospitals and other healthcare facilities disclose transgender youth and adults' complete and identifiable medical and billing records. We have attached a copy of the report for your benefit. These thinly veiled political assaults come at the expense of vulnerable patients. We are concerned that hospitals are feebly complying with AGs' requests, betraying their obligation to protect patient privacy.

Some hospitals have exercised all the tools and legal avenues at their disposal to protect patient privacy. The actions of Washington University in St. Louis (WashU) and Seattle Children's Hospital (SCH) represent best practices in protecting the private, identifiable medical information of transgender youth and adults. Both hospitals pushed back against the AGs' requests in court, challenging that the AGs abused their authority by going beyond their jurisdiction. WashU asserts that the Missouri AG is not the state's health oversight actor and SCH's position is that the Texas AG's jurisdiction does not extend to Washington State. To date, WashU and SCH have refused to disclose identifiable medical information except when ordered by a court.

In contrast, other hospitals have acted with disregard for their patients' safety and wellbeing. Vanderbilt University Medical Center (VUMC) not only failed to protect its patients, but it negligently harmed some of them. In response to an administrative request from the Tennessee AG, VUMC turned over tens of thousands of pages of medical and billing records to the Tennessee AG. These records, which VUMC turned over without a court order as part of a Medicaid fraud billing investigation, include pictures of intimate body parts, photographs that were intended for medical decision-making and clinical planning.

VUMC did not require the Tennessee AG to clearly demonstrate its need for such information. Moreover, VUMC did not inform patients about its disclosure of their fully identifiable, non-redacted medical records. The hospital only notified patients months later, after the Tennessee AG's demands were revealed in a public lawsuit. VUMC then notified and misnotified patients, including improperly notifying some that their records had been shared with the Tennessee AG when they had, in fact, been requested but not shared. The devastating impact of patient medical record disclosures in Tennessee — which led to patients experiencing suicidal ideation — have demonstrated the unimaginable and extensive harms that occur when hospitals fail to protect patient privacy. Further, VUMC now faces a lawsuit from patients, who are seeking class certification on behalf

of all clinic patients who were impacted by VUMC notification or record disclosures, accusing the hospital of negligence and violating their privacy.

Many Americans are familiar with the Health Insurance Portability and Accountability Act (HIPAA), often described as a health privacy law, because of their interactions with patient consent disclosure paperwork in the doctor's office. Congress passed HIPAA in 1996 and gave the Department of Health and Human Services (HHS) the authority to issue broad regulations to secure Americans' health privacy. However, HHS' rules currently provide Americans with fewer privacy protections against law enforcement demands for their health records than Federal Courts have held they have for their emails, text messages, or location data. HIPAA does not require a court order for law enforcement demands for patient records from covered entities — health plans, health care administrators, and healthcare providers — but the law sets conditions that must be met before covered entities can hand over identifiable patient records. Section 164.512(f)(1)(ii) of the HIPAA Privacy Rule permits law enforcement agencies to obtain patient information with a mere subpoena or administrative request, and Section 164.512(e) allows for government health oversight entities to demand patient information pursuant to an administrative request or judicial proceeding. HIPAA permits hospitals to disclose protected health information to law enforcement officials in response to an administrative request if the requested information is relevant and material to the investigation, and specific and limited in scope, and de-identified information could not reasonably be used.

HIPAA only sets the minimum standards covered entities must meet to safeguard patient information. Organizations have opportunities to push back against law enforcement requests for patient information and to tell patients when their records are disclosed to law enforcement. Though HHS' rules permit hospitals to comply with law enforcement demands without scrutinizing the demanding entity's compliance with the three-part-test described above, healthcare providers have an ethical duty and should go well beyond the letter of the law to put patient privacy first. Hospitals must act to protect Americans from the harm caused by state AGs who have weaponized their legal authority against the transgender community. It is only a matter of time before AGs expand the use of the surveillance tools to target others seeking necessary medical care, like abortion care.

In the wake of the *Dobbs* decision, Congressional Democrats urged HHS to update the HIPAA privacy rule to protect Americans' health records from warrantless law enforcement disclosures. In April of last year, HHS announced a draft update to the HIPAA Privacy Rule, which offered some modest, but insufficient protections for reproductive health data by creating a hard-to-enforce certification structure and not taking into account secondary use of medical records or data. Forty-seven members of Congress called on HHS to go further to require a warrant for Americans' medical record releases to law enforcement and to close these other policy gaps. In December, Chairman Wyden along with Representatives Jayapal and Jacobs sent a letter to HHS detailing the findings of an oversight inquiry into the inadequate pharmacy privacy practices at eight major pharmacy chains. None of the surveyed pharmacies require a warrant prior to sharing prescription records with law enforcement, and some pharmacies do not even require legal professionals to review medical record demands. Further, only one pharmacy requires patient notification following law enforcement disclosures.

Until HHS acts to raise the bar on patient privacy, patients will look to their providers and their affiliated hospitals to ensure that their intimate health information is safe. The ethical foundations of privacy laws, such as HIPAA, mirror the same fundamental principles of healthcare professionalism and the doctor-patient relationship, like trust, respect for autonomy, and fidelity. As a leader and a convener of hospitals, your hospital association is best positioned to make sure its members are appropriately safeguarding patient privacy by establishing and disseminating best practices for medical privacy to safeguard against future bad faith investigations.

Hospitals should proactively protect sensitive, patient-identifiable information. The significant increase in debilitating cyberattacks against hospitals and other parts of the healthcare ecosystem, such as the recent Change Healthcare fiasco, highlights the need for sound data security practices. As the National Institute for Standards and Technology (NIST) has noted, "[t]he likelihood of harm caused by a breach involving [Personal Identifiable Information (PII)] is greatly reduced if an organization minimizes the amount of PII it uses, collects, and stores." **Hospitals should consider implementing data minimization and destruction policies** that protect patients from foreseeable harm caused by health data breaches. Further, **hospital administrators should establish policies and procedures to respond to legal demands**, including from law enforcement agencies, so that hospitals are equipped to respond in a manner that safeguards patient privacy.

There are clear best practices to protect patient privacy that hospitals should implement once they receive legal demands. **Hospitals should insist on a higher legal standard in response to demands by law enforcement for unredacted patient medical records**, as WashU and SCH did, when they have a good-faith legal rationale for doing so. This mirrors the approach taken by technology companies to protect the privacy of their customers' communications. In 2010, after a federal court of appeals held that Americans have a reasonable expectation of privacy in their emails, and that the 1986 law permitting disclosures of email pursuant to a subpoena was unconstitutional, all major free email providers started requiring a warrant prior to disclosing such data – nationwide. By applying a single appeals court decision across the country, the email provider industry acted on its own to respond to the courts and successfully raised the threshold for the legal process required to access Americans' emails.

Just as SCH refused to comply with the Texas AG's request for its medical records, **hospitals should closely review whether an out-of-state AG has any legal authority to demand medical records beyond its state border.** Because out-of-state demands raise troubling legal concerns, hospitals should pursue judicial review of these demands to ensure they comply with state and federal law and the Constitution, including heightened scrutiny of the demand under a state's shield law, if applicable, that would demand a higher standard of protection for patient records. A similar system already exists for requests from foreign governments: these demands are routed to the Department of Justice for verification and compliance with the law. Likewise, **hospitals should consider referring out-of-state demands to their state AG's office when their state AG has a demonstrated track record of protecting patient privacy**, so that they may work in partnership to evaluate the claim. This practice will also minimize the resource strain that some hospitals may face in pushing back against these types of demands.

In the event of patient record disclosures, absent a non-disclosure or "gag" order issued by a judge, **hospitals should proactively and promptly notify patients about record disclosures to law enforcement entities and AGs**. Further, all **hospitals should require law enforcement to provide specific and detailed supporting information for having satisfied the three-part test for receiving identifiable patient information, prior to sharing any patients' medical information.** Hospitals should refuse to hand over medical information in response to demands that merely rephrase the three-part test in the affirmative.

We are pursuing an all-of-the-above effort to shore-up the health privacy of Americans: we're conducting oversight, we're pushing HHS to improve privacy regulations, and now we're asking hospitals and their associations to do their part to protect patients' privacy rights. Your hospital association has the know-how to establish and spread best practices throughout the healthcare industry. Your position – with open communication channels to hospitals throughout the nation – and an established role as a trusted guide to your members, makes your hospital association the logical stakeholder to take up this task. We urge you this calendar year to establish best practices for patient privacy, schedule a roundtable where relevant stakeholders, including

policymakers, can develop best practices, and create a resource toolkit to assist hospitals in pushing back against invasive medical record requests.

Our ultimate goal is to prepare hospitals to use the levers already at their disposal, through HIPAA, to better safeguard the privacy and dignity of trans patients. We look forward to working with you on this important issue.

Sincerely,

Ron Wyden
United States Senator

Bernard Sanders
United States Senator

Sara Jacobs
Member of Congress

Tammy Baldwin
United States Senator

Pramila Jayapal
Member of Congress

Mazie K. Hirono
United States Senator

Mark Pocan
Member of Congress

Jeffrey A. Merkley
United States Senator

Mark Takano
Member of Congress

Sheldon Whitehouse
United States Senator

Elizabeth Warren
United States Senator

Martin Heinrich
United States Senator

Chris Van Hollen
United States Senator

Alex Padilla
United States Senator

Becca Balint
Member of Congress

Robert Garcia
Member of Congress

Rosa L. DeLauro
Member of Congress

James P. McGovern
Member of Congress

Alexandria Ocasio-Cortez
Member of Congress

Brian Schatz
United States Senator

Adam B. Schiff
Member of Congress

Edward J. Markey
United States Senator

Maxwell Alejandro Frost
Member of Congress

Peter Welch
United States Senator

Zoe Lofgren
Member of Congress

Barbara Lee
Member of Congress

Rashida Tlaib
Member of Congress

Anna G. Eshoo
Member of Congress

Summer Lee
Member of Congress

Ayanna Pressley
Member of Congress

Suzanne Bonamici
Member of Congress

Val Hoyle
Member of Congress

Eleanor Holmes Norton
Member of Congress

Cori Bush
Member of Congress

Sylvia R. Garcia
Member of Congress

Raúl M. Grijalva
Member of Congress

Andrea Salinas
Member of Congress

Jasmine Crockett
Member of Congress

Nikema Williams
Member of Congress

Jared Huffman
Member of Congress

Valerie P. Foushee
Member of Congress

Stephen F. Lynch
Member of Congress

Ted W. Lieu
Member of Congress

Congress of the United States

Washington, DC 20515

April 16, 2024

Richard J. Pollack
President and CEO
American Hospital Association
800 10th Street, NW – 2 City Center, Suite 400
Washington, DC 20001

Dear Mr. Pollack:

We write to request that you urge your member hospitals to protect American patients' medical privacy from abusive legal demands by state attorneys general (AGs). According to a recent Senate Finance Committee Majority Staff Report entitled, "How State Attorneys General Target Transgender Youth and Adults by Weaponizing the Medicaid Program and their Health Oversight Authority" state-level politicians are abusing their legal authority to attack transgender patients for political gain, while undermining faith in the Medicaid program. In at least four states, AGs have abused their legal powers to demand that hospitals and other healthcare facilities disclose transgender youth and adults' complete and identifiable medical and billing records. We have attached a copy of the report for your benefit. These thinly veiled political assaults come at the expense of vulnerable patients. We are concerned that hospitals are feebly complying with AGs' requests, betraying their obligation to protect patient privacy.

Some hospitals have exercised all the tools and legal avenues at their disposal to protect patient privacy. The actions of Washington University in St. Louis (WashU) and Seattle Children's Hospital (SCH) represent best practices in protecting the private, identifiable medical information of transgender youth and adults. Both hospitals pushed back against the AGs' requests in court, challenging that the AGs abused their authority by going beyond their jurisdiction. WashU asserts that the Missouri AG is not the state's health oversight actor and SCH's position is that the Texas AG's jurisdiction does not extend to Washington State. To date, WashU and SCH have refused to disclose identifiable medical information except when ordered by a court.

In contrast, other hospitals have acted with disregard for their patients' safety and wellbeing. Vanderbilt University Medical Center (VUMC) not only failed to protect its patients, but it negligently harmed some of them. In response to an administrative request from the Tennessee AG, VUMC turned over tens of thousands of pages of medical and billing records to the Tennessee AG. These records, which VUMC turned over without a court order as part of a Medicaid fraud billing investigation, include pictures of intimate body parts, photographs that were intended for medical decision-making and clinical planning.

VUMC did not require the Tennessee AG to clearly demonstrate its need for such information. Moreover, VUMC did not inform patients about its disclosure of their fully identifiable, non-redacted medical records. The hospital only notified patients months later, after the Tennessee AG's demands were revealed in a public lawsuit. VUMC then notified and misnotified patients, including improperly notifying some that their records had been shared with the Tennessee AG when they had, in fact, been requested but not shared. The devastating impact of patient medical record disclosures in Tennessee — which led to patients experiencing suicidal ideation — have demonstrated the unimaginable and extensive harms that occur when hospitals fail to protect patient privacy. Further, VUMC now faces a lawsuit from patients, who are seeking class certification on behalf

of all clinic patients who were impacted by VUMC notification or record disclosures, accusing the hospital of negligence and violating their privacy.

Many Americans are familiar with the Health Insurance Portability and Accountability Act (HIPAA), often described as a health privacy law, because of their interactions with patient consent disclosure paperwork in the doctor's office. Congress passed HIPAA in 1996 and gave the Department of Health and Human Services (HHS) the authority to issue broad regulations to secure Americans' health privacy. However, HHS' rules currently provide Americans with fewer privacy protections against law enforcement demands for their health records than Federal Courts have held they have for their emails, text messages, or location data. HIPAA does not require a court order for law enforcement demands for patient records from covered entities — health plans, health care administrators, and healthcare providers — but the law sets conditions that must be met before covered entities can hand over identifiable patient records. Section 164.512(f)(1)(ii) of the HIPAA Privacy Rule permits law enforcement agencies to obtain patient information with a mere subpoena or administrative request, and Section 164.512(e) allows for government health oversight entities to demand patient information pursuant to an administrative request or judicial proceeding. HIPAA permits hospitals to disclose protected health information to law enforcement officials in response to an administrative request if the requested information is relevant and material to the investigation, and specific and limited in scope, and de-identified information could not reasonably be used.

HIPAA only sets the minimum standards covered entities must meet to safeguard patient information. Organizations have opportunities to push back against law enforcement requests for patient information and to tell patients when their records are disclosed to law enforcement. Though HHS' rules permit hospitals to comply with law enforcement demands without scrutinizing the demanding entity's compliance with the three-part-test described above, healthcare providers have an ethical duty and should go well beyond the letter of the law to put patient privacy first. Hospitals must act to protect Americans from the harm caused by state AGs who have weaponized their legal authority against the transgender community. It is only a matter of time before AGs expand the use of the surveillance tools to target others seeking necessary medical care, like abortion care.

In the wake of the *Dobbs* decision, Congressional Democrats urged HHS to update the HIPAA privacy rule to protect Americans' health records from warrantless law enforcement disclosures. In April of last year, HHS announced a draft update to the HIPAA Privacy Rule, which offered some modest, but insufficient protections for reproductive health data by creating a hard-to-enforce certification structure and not taking into account secondary use of medical records or data. Forty-seven members of Congress called on HHS to go further to require a warrant for Americans' medical record releases to law enforcement and to close these other policy gaps. In December, Chairman Wyden along with Representatives Jayapal and Jacobs sent a letter to HHS detailing the findings of an oversight inquiry into the inadequate pharmacy privacy practices at eight major pharmacy chains. None of the surveyed pharmacies require a warrant prior to sharing prescription records with law enforcement, and some pharmacies do not even require legal professionals to review medical record demands. Further, only one pharmacy requires patient notification following law enforcement disclosures.

Until HHS acts to raise the bar on patient privacy, patients will look to their providers and their affiliated hospitals to ensure that their intimate health information is safe. The ethical foundations of privacy laws, such as HIPAA, mirror the same fundamental principles of healthcare professionalism and the doctor-patient relationship, like trust, respect for autonomy, and fidelity. As a leader and a convener of hospitals, your hospital association is best positioned to make sure its members are appropriately safeguarding patient privacy by establishing and disseminating best practices for medical privacy to safeguard against future bad faith investigations.

Hospitals should proactively protect sensitive, patient-identifiable information. The significant increase in debilitating cyberattacks against hospitals and other parts of the healthcare ecosystem, such as the recent Change Healthcare fiasco, highlights the need for sound data security practices. As the National Institute for Standards and Technology (NIST) has noted, "[t]he likelihood of harm caused by a breach involving [Personal Identifiable Information (PII)] is greatly reduced if an organization minimizes the amount of PII it uses, collects, and stores." **Hospitals should consider implementing data minimization and destruction policies** that protect patients from foreseeable harm caused by health data breaches. Further, **hospital administrators should establish policies and procedures to respond to legal demands**, including from law enforcement agencies, so that hospitals are equipped to respond in a manner that safeguards patient privacy.

There are clear best practices to protect patient privacy that hospitals should implement once they receive legal demands. **Hospitals should insist on a higher legal standard in response to demands by law enforcement for unredacted patient medical records**, as WashU and SCH did, when they have a good-faith legal rationale for doing so. This mirrors the approach taken by technology companies to protect the privacy of their customers' communications. In 2010, after a federal court of appeals held that Americans have a reasonable expectation of privacy in their emails, and that the 1986 law permitting disclosures of email pursuant to a subpoena was unconstitutional, all major free email providers started requiring a warrant prior to disclosing such data – nationwide. By applying a single appeals court decision across the country, the email provider industry acted on its own to respond to the courts and successfully raised the threshold for the legal process required to access Americans' emails.

Just as SCH refused to comply with the Texas AG's request for its medical records, **hospitals should closely review whether an out-of-state AG has any legal authority to demand medical records beyond its state border.** Because out-of-state demands raise troubling legal concerns, hospitals should pursue judicial review of these demands to ensure they comply with state and federal law and the Constitution, including heightened scrutiny of the demand under a state's shield law, if applicable, that would demand a higher standard of protection for patient records. A similar system already exists for requests from foreign governments: these demands are routed to the Department of Justice for verification and compliance with the law. Likewise, **hospitals should consider referring out-of-state demands to their state AG's office when their state AG has a demonstrated track record of protecting patient privacy**, so that they may work in partnership to evaluate the claim. This practice will also minimize the resource strain that some hospitals may face in pushing back against these types of demands.

In the event of patient record disclosures, absent a non-disclosure or "gag" order issued by a judge, **hospitals should proactively and promptly notify patients about record disclosures to law enforcement entities and AGs**. Further, all **hospitals should require law enforcement to provide specific and detailed supporting information for having satisfied the three-part test for receiving identifiable patient information, prior to sharing any patients' medical information.** Hospitals should refuse to hand over medical information in response to demands that merely rephrase the three-part test in the affirmative.

We are pursuing an all-of-the-above effort to shore-up the health privacy of Americans: we're conducting oversight, we're pushing HHS to improve privacy regulations, and now we're asking hospitals and their associations to do their part to protect patients' privacy rights. Your hospital association has the know-how to establish and spread best practices throughout the healthcare industry. Your position – with open communication channels to hospitals throughout the nation – and an established role as a trusted guide to your members, makes your hospital association the logical stakeholder to take up this task. We urge you this calendar year to establish best practices for patient privacy, schedule a roundtable where relevant stakeholders, including

policymakers, can develop best practices, and create a resource toolkit to assist hospitals in pushing back against invasive medical record requests.

Our ultimate goal is to prepare hospitals to use the levers already at their disposal, through HIPAA, to better safeguard the privacy and dignity of trans patients. We look forward to working with you on this important issue.

Sincerely,

Ron Wyden
United States Senator

Bernard Sanders
United States Senator

Sara Jacobs
Member of Congress

Tammy Baldwin
United States Senator

Pramila Jayapal
Member of Congress

Mazie K. Hirono
United States Senator

Mark Pocan
Member of Congress

Jeffrey A. Merkley
United States Senator

Mark Takano
Member of Congress

Sheldon Whitehouse
United States Senator

Elizabeth Warren
United States Senator

Martin Heinrich
United States Senator

Chris Van Hollen
United States Senator

Alex Padilla
United States Senator

Becca Balint
Member of Congress

Robert Garcia
Member of Congress

Rosa L. DeLauro
Member of Congress

James P. McGovern
Member of Congress

Alexandria Ocasio-Cortez
Member of Congress

Brian Schatz
United States Senator

Adam B. Schiff
Member of Congress

Edward J. Markey
United States Senator

Maxwell Alejandro Frost
Member of Congress

Peter Welch
United States Senator

Zoe Lofgren
Member of Congress

Barbara Lee
Member of Congress

Rashida Tlaib
Member of Congress

Anna G. Eshoo
Member of Congress

Summer Lee
Member of Congress

Ayanna Pressley
Member of Congress

Suzanne Bonamici
Member of Congress

Val Hoyle
Member of Congress

Eleanor Holmes Norton
Member of Congress

Cori Bush
Member of Congress

Sylvia R. Garcia
Member of Congress

Raúl M. Grijalva
Member of Congress

Andrea Salinas
Member of Congress

Jasmine Crockett
Member of Congress

Nikema Williams
Member of Congress

Jared Huffman
Member of Congress

Valerie P. Foushee
Member of Congress

Stephen F. Lynch
Member of Congress

Ted W. Lieu
Member of Congress

Congress of the United States

Washington, DC 20515

April 16, 2024

Matthew Cook
CEO
Children's Hospital Association
600 13th Street, NW, Suite 500
Washington, DC 20005

Dear Mr. Cook:

We write to request that you urge your member hospitals to protect American patients' medical privacy from abusive legal demands by state attorneys general (AGs). According to a recent Senate Finance Committee Majority Staff Report entitled, "How State Attorneys General Target Transgender Youth and Adults by Weaponizing the Medicaid Program and their Health Oversight Authority" state-level politicians are abusing their legal authority to attack transgender patients for political gain, while undermining faith in the Medicaid program. In at least four states, AGs have abused their legal powers to demand that hospitals and other healthcare facilities disclose transgender youth and adults' complete and identifiable medical and billing records. We have attached a copy of the report for your benefit. These thinly veiled political assaults come at the expense of vulnerable patients. We are concerned that hospitals are feebly complying with AGs' requests, betraying their obligation to protect patient privacy.

Some hospitals have exercised all the tools and legal avenues at their disposal to protect patient privacy. The actions of Washington University in St. Louis (WashU) and Seattle Children's Hospital (SCH) represent best practices in protecting the private, identifiable medical information of transgender youth and adults. Both hospitals pushed back against the AGs' requests in court, challenging that the AGs abused their authority by going beyond their jurisdiction. WashU asserts that the Missouri AG is not the state's health oversight actor and SCH's position is that the Texas AG's jurisdiction does not extend to Washington State. To date, WashU and SCH have refused to disclose identifiable medical information except when ordered by a court.

In contrast, other hospitals have acted with disregard for their patients' safety and wellbeing. Vanderbilt University Medical Center (VUMC) not only failed to protect its patients, but it negligently harmed some of them. In response to an administrative request from the Tennessee AG, VUMC turned over tens of thousands of pages of medical and billing records to the Tennessee AG. These records, which VUMC turned over without a court order as part of a Medicaid fraud billing investigation, include pictures of intimate body parts, photographs that were intended for medical decision-making and clinical planning.

VUMC did not require the Tennessee AG to clearly demonstrate its need for such information. Moreover, VUMC did not inform patients about its disclosure of their fully identifiable, non-redacted medical records. The hospital only notified patients months later, after the Tennessee AG's demands were revealed in a public lawsuit. VUMC then notified and misnotified patients, including improperly notifying some that their records had been shared with the Tennessee AG when they had, in fact, been requested but not shared. The devastating impact of patient medical record disclosures in Tennessee — which led to patients experiencing suicidal ideation — have demonstrated the unimaginable and extensive harms that occur when hospitals fail to protect patient privacy. Further, VUMC now faces a lawsuit from patients, who are seeking class certification on behalf

of all clinic patients who were impacted by VUMC notification or record disclosures, accusing the hospital of negligence and violating their privacy.

Many Americans are familiar with the Health Insurance Portability and Accountability Act (HIPAA), often described as a health privacy law, because of their interactions with patient consent disclosure paperwork in the doctor's office. Congress passed HIPAA in 1996 and gave the Department of Health and Human Services (HHS) the authority to issue broad regulations to secure Americans' health privacy. However, HHS' rules currently provide Americans with fewer privacy protections against law enforcement demands for their health records than Federal Courts have held they have for their emails, text messages, or location data. HIPAA does not require a court order for law enforcement demands for patient records from covered entities — health plans, health care administrators, and healthcare providers — but the law sets conditions that must be met before covered entities can hand over identifiable patient records. Section 164.512(f)(1)(ii) of the HIPAA Privacy Rule permits law enforcement agencies to obtain patient information with a mere subpoena or administrative request, and Section 164.512(e) allows for government health oversight entities to demand patient information pursuant to an administrative request or judicial proceeding. HIPAA permits hospitals to disclose protected health information to law enforcement officials in response to an administrative request if the requested information is relevant and material to the investigation, and specific and limited in scope, and de-identified information could not reasonably be used.

HIPAA only sets the minimum standards covered entities must meet to safeguard patient information. Organizations have opportunities to push back against law enforcement requests for patient information and to tell patients when their records are disclosed to law enforcement. Though HHS' rules permit hospitals to comply with law enforcement demands without scrutinizing the demanding entity's compliance with the three-part-test described above, healthcare providers have an ethical duty and should go well beyond the letter of the law to put patient privacy first. Hospitals must act to protect Americans from the harm caused by state AGs who have weaponized their legal authority against the transgender community. It is only a matter of time before AGs expand the use of the surveillance tools to target others seeking necessary medical care, like abortion care.

In the wake of the *Dobbs* decision, Congressional Democrats urged HHS to update the HIPAA privacy rule to protect Americans' health records from warrantless law enforcement disclosures. In April of last year, HHS announced a draft update to the HIPAA Privacy Rule, which offered some modest, but insufficient protections for reproductive health data by creating a hard-to-enforce certification structure and not taking into account secondary use of medical records or data. Forty-seven members of Congress called on HHS to go further to require a warrant for Americans' medical record releases to law enforcement and to close these other policy gaps. In December, Chairman Wyden along with Representatives Jayapal and Jacobs sent a letter to HHS detailing the findings of an oversight inquiry into the inadequate pharmacy privacy practices at eight major pharmacy chains. None of the surveyed pharmacies require a warrant prior to sharing prescription records with law enforcement, and some pharmacies do not even require legal professionals to review medical record demands. Further, only one pharmacy requires patient notification following law enforcement disclosures.

Until HHS acts to raise the bar on patient privacy, patients will look to their providers and their affiliated hospitals to ensure that their intimate health information is safe. The ethical foundations of privacy laws, such as HIPAA, mirror the same fundamental principles of healthcare professionalism and the doctor-patient relationship, like trust, respect for autonomy, and fidelity. As a leader and a convener of hospitals, your hospital association is best positioned to make sure its members are appropriately safeguarding patient privacy by establishing and disseminating best practices for medical privacy to safeguard against future bad faith investigations.

Hospitals should proactively protect sensitive, patient-identifiable information. The significant increase in debilitating cyberattacks against hospitals and other parts of the healthcare ecosystem, such as the recent Change Healthcare fiasco, highlights the need for sound data security practices. As the National Institute for Standards and Technology (NIST) has noted, "[t]he likelihood of harm caused by a breach involving [Personal Identifiable Information (PII)] is greatly reduced if an organization minimizes the amount of PII it uses, collects, and stores." **Hospitals should consider implementing data minimization and destruction policies** that protect patients from foreseeable harm caused by health data breaches. Further, **hospital administrators should establish policies and procedures to respond to legal demands**, including from law enforcement agencies, so that hospitals are equipped to respond in a manner that safeguards patient privacy.

There are clear best practices to protect patient privacy that hospitals should implement once they receive legal demands. **Hospitals should insist on a higher legal standard in response to demands by law enforcement for unredacted patient medical records**, as WashU and SCH did, when they have a good-faith legal rationale for doing so. This mirrors the approach taken by technology companies to protect the privacy of their customers' communications. In 2010, after a federal court of appeals held that Americans have a reasonable expectation of privacy in their emails, and that the 1986 law permitting disclosures of email pursuant to a subpoena was unconstitutional, all major free email providers started requiring a warrant prior to disclosing such data – nationwide. By applying a single appeals court decision across the country, the email provider industry acted on its own to respond to the courts and successfully raised the threshold for the legal process required to access Americans' emails.

Just as SCH refused to comply with the Texas AG's request for its medical records, **hospitals should closely review whether an out-of-state AG has any legal authority to demand medical records beyond its state border.** Because out-of-state demands raise troubling legal concerns, hospitals should pursue judicial review of these demands to ensure they comply with state and federal law and the Constitution, including heightened scrutiny of the demand under a state's shield law, if applicable, that would demand a higher standard of protection for patient records. A similar system already exists for requests from foreign governments: these demands are routed to the Department of Justice for verification and compliance with the law. Likewise, **hospitals should consider referring out-of-state demands to their state AG's office when their state AG has a demonstrated track record of protecting patient privacy**, so that they may work in partnership to evaluate the claim. This practice will also minimize the resource strain that some hospitals may face in pushing back against these types of demands.

In the event of patient record disclosures, absent a non-disclosure or "gag" order issued by a judge, **hospitals should proactively and promptly notify patients about record disclosures to law enforcement entities and AGs**. Further, all **hospitals should require law enforcement to provide specific and detailed supporting information for having satisfied the three-part test for receiving identifiable patient information, prior to sharing any patients' medical information.** Hospitals should refuse to hand over medical information in response to demands that merely rephrase the three-part test in the affirmative.

We are pursuing an all-of-the-above effort to shore-up the health privacy of Americans: we're conducting oversight, we're pushing HHS to improve privacy regulations, and now we're asking hospitals and their associations to do their part to protect patients' privacy rights. Your hospital association has the know-how to establish and spread best practices throughout the healthcare industry. Your position – with open communication channels to hospitals throughout the nation – and an established role as a trusted guide to your members, makes your hospital association the logical stakeholder to take up this task. We urge you this calendar year to establish best practices for patient privacy, schedule a roundtable where relevant stakeholders, including

policymakers, can develop best practices, and create a resource toolkit to assist hospitals in pushing back against invasive medical record requests.

Our ultimate goal is to prepare hospitals to use the levers already at their disposal, through HIPAA, to better safeguard the privacy and dignity of trans patients. We look forward to working with you on this important issue.

Sincerely,

Ron Wyden
United States Senator

Bernard Sanders
United States Senator

Sara Jacobs
Member of Congress

Tammy Baldwin
United States Senator

Pramila Jayapal
Member of Congress

Mazie K. Hirono
United States Senator

Mark Pocan
Member of Congress

Jeffrey A. Merkley
United States Senator

Mark Takano
Member of Congress

Sheldon Whitehouse
United States Senator

Elizabeth Warren
United States Senator

Martin Heinrich
United States Senator

Chris Van Hollen
United States Senator

Alex Padilla
United States Senator

Becca Balint
Member of Congress

Robert Garcia
Member of Congress

Rosa L. DeLauro
Member of Congress

James P. McGovern
Member of Congress

Alexandria Ocasio-Cortez
Member of Congress

Brian Schatz
United States Senator

Adam B. Schiff
Member of Congress

Edward J. Markey
United States Senator

Maxwell Alejandro Frost
Member of Congress

Peter Welch
United States Senator

Zoe Lofgren
Member of Congress

Barbara Lee
Member of Congress

Rashida Tlaib
Member of Congress

Anna G. Eshoo
Member of Congress

Summer Lee
Member of Congress

Ayanna Pressley
Member of Congress

Suzanne Bonamici
Member of Congress

Val Hoyle
Member of Congress

Eleanor Holmes Norton
Member of Congress

Cori Bush
Member of Congress

Sylvia R. Garcia
Member of Congress

Raúl M. Grijalva
Member of Congress

Andrea Salinas
Member of Congress

Jasmine Crockett
Member of Congress

Nikema Williams
Member of Congress

Jared Huffman
Member of Congress

Valerie P. Foushee
Member of Congress

Stephen F. Lynch
Member of Congress

Ted W. Lieu
Member of Congress

Congress of the United States

Washington, DC 20515

April 16, 2024

Charles "Chip" N. Kahn III
President and CEO
Federation of American Hospitals
750 9th Street, NW, Suite 600
Washington, DC 20001

Dear Mr. Kahn:

We write to request that you urge your member hospitals to protect American patients' medical privacy from abusive legal demands by state attorneys general (AGs). According to a recent Senate Finance Committee Majority Staff Report entitled, "How State Attorneys General Target Transgender Youth and Adults by Weaponizing the Medicaid Program and their Health Oversight Authority" state-level politicians are abusing their legal authority to attack transgender patients for political gain, while undermining faith in the Medicaid program. In at least four states, AGs have abused their legal powers to demand that hospitals and other healthcare facilities disclose transgender youth and adults' complete and identifiable medical and billing records. We have attached a copy of the report for your benefit. These thinly veiled political assaults come at the expense of vulnerable patients. We are concerned that hospitals are feebly complying with AGs' requests, betraying their obligation to protect patient privacy.

Some hospitals have exercised all the tools and legal avenues at their disposal to protect patient privacy. The actions of Washington University in St. Louis (WashU) and Seattle Children's Hospital (SCH) represent best practices in protecting the private, identifiable medical information of transgender youth and adults. Both hospitals pushed back against the AGs' requests in court, challenging that the AGs abused their authority by going beyond their jurisdiction. WashU asserts that the Missouri AG is not the state's health oversight actor and SCH's position is that the Texas AG's jurisdiction does not extend to Washington State. To date, WashU and SCH have refused to disclose identifiable medical information except when ordered by a court.

In contrast, other hospitals have acted with disregard for their patients' safety and wellbeing. Vanderbilt University Medical Center (VUMC) not only failed to protect its patients, but it negligently harmed some of them. In response to an administrative request from the Tennessee AG, VUMC turned over tens of thousands of pages of medical and billing records to the Tennessee AG. These records, which VUMC turned over without a court order as part of a Medicaid fraud billing investigation, include pictures of intimate body parts, photographs that were intended for medical decision-making and clinical planning.

VUMC did not require the Tennessee AG to clearly demonstrate its need for such information. Moreover, VUMC did not inform patients about its disclosure of their fully identifiable, non-redacted medical records. The hospital only notified patients months later, after the Tennessee AG's demands were revealed in a public lawsuit. VUMC then notified and misnotified patients, including improperly notifying some that their records had been shared with the Tennessee AG when they had, in fact, been requested but not shared. The devastating impact of patient medical record disclosures in Tennessee — which led to patients experiencing suicidal ideation — have demonstrated the unimaginable and extensive harms that occur when hospitals fail to protect patient privacy. Further, VUMC now faces a lawsuit from patients, who are seeking class certification on behalf

of all clinic patients who were impacted by VUMC notification or record disclosures, accusing the hospital of negligence and violating their privacy.

Many Americans are familiar with the Health Insurance Portability and Accountability Act (HIPAA), often described as a health privacy law, because of their interactions with patient consent disclosure paperwork in the doctor's office. Congress passed HIPAA in 1996 and gave the Department of Health and Human Services (HHS) the authority to issue broad regulations to secure Americans' health privacy. However, HHS' rules currently provide Americans with fewer privacy protections against law enforcement demands for their health records than Federal Courts have held they have for their emails, text messages, or location data. HIPAA does not require a court order for law enforcement demands for patient records from covered entities — health plans, health care administrators, and healthcare providers — but the law sets conditions that must be met before covered entities can hand over identifiable patient records. Section 164.512(f)(1)(ii) of the HIPAA Privacy Rule permits law enforcement agencies to obtain patient information with a mere subpoena or administrative request, and Section 164.512(e) allows for government health oversight entities to demand patient information pursuant to an administrative request or judicial proceeding. HIPAA permits hospitals to disclose protected health information to law enforcement officials in response to an administrative request if the requested information is relevant and material to the investigation, and specific and limited in scope, and de-identified information could not reasonably be used.

HIPAA only sets the minimum standards covered entities must meet to safeguard patient information. Organizations have opportunities to push back against law enforcement requests for patient information and to tell patients when their records are disclosed to law enforcement. Though HHS' rules permit hospitals to comply with law enforcement demands without scrutinizing the demanding entity's compliance with the three-part-test described above, healthcare providers have an ethical duty and should go well beyond the letter of the law to put patient privacy first. Hospitals must act to protect Americans from the harm caused by state AGs who have weaponized their legal authority against the transgender community. It is only a matter of time before AGs expand the use of the surveillance tools to target others seeking necessary medical care, like abortion care.

In the wake of the *Dobbs* decision, Congressional Democrats urged HHS to update the HIPAA privacy rule to protect Americans' health records from warrantless law enforcement disclosures. In April of last year, HHS announced a draft update to the HIPAA Privacy Rule, which offered some modest, but insufficient protections for reproductive health data by creating a hard-to-enforce certification structure and not taking into account secondary use of medical records or data. Forty-seven members of Congress called on HHS to go further to require a warrant for Americans' medical record releases to law enforcement and to close these other policy gaps. In December, Chairman Wyden along with Representatives Jayapal and Jacobs sent a letter to HHS detailing the findings of an oversight inquiry into the inadequate pharmacy privacy practices at eight major pharmacy chains. None of the surveyed pharmacies require a warrant prior to sharing prescription records with law enforcement, and some pharmacies do not even require legal professionals to review medical record demands. Further, only one pharmacy requires patient notification following law enforcement disclosures.

Until HHS acts to raise the bar on patient privacy, patients will look to their providers and their affiliated hospitals to ensure that their intimate health information is safe. The ethical foundations of privacy laws, such as HIPAA, mirror the same fundamental principles of healthcare professionalism and the doctor-patient relationship, like trust, respect for autonomy, and fidelity. As a leader and a convener of hospitals, your hospital association is best positioned to make sure its members are appropriately safeguarding patient privacy by establishing and disseminating best practices for medical privacy to safeguard against future bad faith investigations.

Hospitals should proactively protect sensitive, patient-identifiable information. The significant increase in debilitating cyberattacks against hospitals and other parts of the healthcare ecosystem, such as the recent Change Healthcare fiasco, highlights the need for sound data security practices. As the National Institute for Standards and Technology (NIST) has noted, "[t]he likelihood of harm caused by a breach involving [Personal Identifiable Information (PII)] is greatly reduced if an organization minimizes the amount of PII it uses, collects, and stores." **Hospitals should consider implementing data minimization and destruction policies** that protect patients from foreseeable harm caused by health data breaches. Further, **hospital administrators should establish policies and procedures to respond to legal demands**, including from law enforcement agencies, so that hospitals are equipped to respond in a manner that safeguards patient privacy.

There are clear best practices to protect patient privacy that hospitals should implement once they receive legal demands. **Hospitals should insist on a higher legal standard in response to demands by law enforcement for unredacted patient medical records**, as WashU and SCH did, when they have a good-faith legal rationale for doing so. This mirrors the approach taken by technology companies to protect the privacy of their customers' communications. In 2010, after a federal court of appeals held that Americans have a reasonable expectation of privacy in their emails, and that the 1986 law permitting disclosures of email pursuant to a subpoena was unconstitutional, all major free email providers started requiring a warrant prior to disclosing such data – nationwide. By applying a single appeals court decision across the country, the email provider industry acted on its own to respond to the courts and successfully raised the threshold for the legal process required to access Americans' emails.

Just as SCH refused to comply with the Texas AG's request for its medical records, **hospitals should closely review whether an out-of-state AG has any legal authority to demand medical records beyond its state border.** Because out-of-state demands raise troubling legal concerns, hospitals should pursue judicial review of these demands to ensure they comply with state and federal law and the Constitution, including heightened scrutiny of the demand under a state's shield law, if applicable, that would demand a higher standard of protection for patient records. A similar system already exists for requests from foreign governments: these demands are routed to the Department of Justice for verification and compliance with the law. Likewise, **hospitals should consider referring out-of-state demands to their state AG's office when their state AG has a demonstrated track record of protecting patient privacy**, so that they may work in partnership to evaluate the claim. This practice will also minimize the resource strain that some hospitals may face in pushing back against these types of demands.

In the event of patient record disclosures, absent a non-disclosure or "gag" order issued by a judge, **hospitals should proactively and promptly notify patients about record disclosures to law enforcement entities and AGs**. Further, all **hospitals should require law enforcement to provide specific and detailed supporting information for having satisfied the three-part test for receiving identifiable patient information, prior to sharing any patients' medical information.** Hospitals should refuse to hand over medical information in response to demands that merely rephrase the three-part test in the affirmative.

We are pursuing an all-of-the-above effort to shore-up the health privacy of Americans: we're conducting oversight, we're pushing HHS to improve privacy regulations, and now we're asking hospitals and their associations to do their part to protect patients' privacy rights. Your hospital association has the know-how to establish and spread best practices throughout the healthcare industry. Your position – with open communication channels to hospitals throughout the nation – and an established role as a trusted guide to your members, makes your hospital association the logical stakeholder to take up this task. We urge you this calendar year to establish best practices for patient privacy, schedule a roundtable where relevant stakeholders, including

policymakers, can develop best practices, and create a resource toolkit to assist hospitals in pushing back against invasive medical record requests.

Our ultimate goal is to prepare hospitals to use the levers already at their disposal, through HIPAA, to better safeguard the privacy and dignity of trans patients. We look forward to working with you on this important issue.

Sincerely,

Ron Wyden
United States Senator

Bernard Sanders
United States Senator

Sara Jacobs
Member of Congress

Tammy Baldwin
United States Senator

Pramila Jayapal
Member of Congress

Mazie K. Hirono
United States Senator

Mark Pocan
Member of Congress

Jeffrey A. Merkley
United States Senator

Mark Takano
Member of Congress

Sheldon Whitehouse
United States Senator

Elizabeth Warren
United States Senator

Martin Heinrich
United States Senator

Chris Van Hollen
United States Senator

Alex Padilla
United States Senator

Becca Balint
Member of Congress

Robert Garcia
Member of Congress

Rosa L. DeLauro
Member of Congress

James P. McGovern
Member of Congress

Alexandria Ocasio-Cortez
Member of Congress

Brian Schatz
United States Senator

Adam B. Schiff
Member of Congress

Edward J. Markey
United States Senator

Maxwell Alejandro Frost
Member of Congress

Peter Welch
United States Senator

Zoe Lofgren
Member of Congress

Barbara Lee
Member of Congress

Rashida Tlaib
Member of Congress

Anna G. Eshoo
Member of Congress

Summer Lee
Member of Congress

Ayanna Pressley
Member of Congress

Suzanne Bonamici
Member of Congress

Val Hoyle
Member of Congress

Eleanor Holmes Norton
Member of Congress

Cori Bush
Member of Congress

Sylvia R. Garcia
Member of Congress

Raúl M. Grijalva
Member of Congress

Andrea Salinas
Member of Congress

Jasmine Crockett
Member of Congress

Nikema Williams
Member of Congress

Jared Huffman
Member of Congress

Valerie P. Foushee
Member of Congress

Stephen F. Lynch
Member of Congress

Ted W. Lieu
Member of Congress

Congress of the United States

Washington, DC 20515

April 16, 2024

Alan Morgan
CEO
National Rural Health Association
50 F Street, NW, Suite 520
Washington, DC 20001

Dear Mr. Morgan:

We write to request that you urge your member hospitals to protect American patients' medical privacy from abusive legal demands by state attorneys general (AGs). According to a recent Senate Finance Committee Majority Staff Report entitled, "How State Attorneys General Target Transgender Youth and Adults by Weaponizing the Medicaid Program and their Health Oversight Authority" state-level politicians are abusing their legal authority to attack transgender patients for political gain, while undermining faith in the Medicaid program. In at least four states, AGs have abused their legal powers to demand that hospitals and other healthcare facilities disclose transgender youth and adults' complete and identifiable medical and billing records. We have attached a copy of the report for your benefit. These thinly veiled political assaults come at the expense of vulnerable patients. We are concerned that hospitals are feebly complying with AGs' requests, betraying their obligation to protect patient privacy.

Some hospitals have exercised all the tools and legal avenues at their disposal to protect patient privacy. The actions of Washington University in St. Louis (WashU) and Seattle Children's Hospital (SCH) represent best practices in protecting the private, identifiable medical information of transgender youth and adults. Both hospitals pushed back against the AGs' requests in court, challenging that the AGs abused their authority by going beyond their jurisdiction. WashU asserts that the Missouri AG is not the state's health oversight actor and SCH's position is that the Texas AG's jurisdiction does not extend to Washington State. To date, WashU and SCH have refused to disclose identifiable medical information except when ordered by a court.

In contrast, other hospitals have acted with disregard for their patients' safety and wellbeing. Vanderbilt University Medical Center (VUMC) not only failed to protect its patients, but it negligently harmed some of them. In response to an administrative request from the Tennessee AG, VUMC turned over tens of thousands of pages of medical and billing records to the Tennessee AG. These records, which VUMC turned over without a court order as part of a Medicaid fraud billing investigation, include pictures of intimate body parts, photographs that were intended for medical decision-making and clinical planning.

VUMC did not require the Tennessee AG to clearly demonstrate its need for such information. Moreover, VUMC did not inform patients about its disclosure of their fully identifiable, non-redacted medical records. The hospital only notified patients months later, after the Tennessee AG's demands were revealed in a public lawsuit. VUMC then notified and misnotified patients, including improperly notifying some that their records had been shared with the Tennessee AG when they had, in fact, been requested but not shared. The devastating impact of patient medical record disclosures in Tennessee — which led to patients experiencing suicidal ideation — have demonstrated the unimaginable and extensive harms that occur when hospitals fail to protect patient privacy. Further, VUMC now faces a lawsuit from patients, who are seeking class certification on behalf

of all clinic patients who were impacted by VUMC notification or record disclosures, accusing the hospital of negligence and violating their privacy.

Many Americans are familiar with the Health Insurance Portability and Accountability Act (HIPAA), often described as a health privacy law, because of their interactions with patient consent disclosure paperwork in the doctor's office. Congress passed HIPAA in 1996 and gave the Department of Health and Human Services (HHS) the authority to issue broad regulations to secure Americans' health privacy. However, HHS' rules currently provide Americans with fewer privacy protections against law enforcement demands for their health records than Federal Courts have held they have for their emails, text messages, or location data. HIPAA does not require a court order for law enforcement demands for patient records from covered entities — health plans, health care administrators, and healthcare providers — but the law sets conditions that must be met before covered entities can hand over identifiable patient records. Section 164.512(f)(1)(ii) of the HIPAA Privacy Rule permits law enforcement agencies to obtain patient information with a mere subpoena or administrative request, and Section 164.512(e) allows for government health oversight entities to demand patient information pursuant to an administrative request or judicial proceeding. HIPAA permits hospitals to disclose protected health information to law enforcement officials in response to an administrative request if the requested information is relevant and material to the investigation, and specific and limited in scope, and de-identified information could not reasonably be used.

HIPAA only sets the minimum standards covered entities must meet to safeguard patient information. Organizations have opportunities to push back against law enforcement requests for patient information and to tell patients when their records are disclosed to law enforcement. Though HHS' rules permit hospitals to comply with law enforcement demands without scrutinizing the demanding entity's compliance with the three-part-test described above, healthcare providers have an ethical duty and should go well beyond the letter of the law to put patient privacy first. Hospitals must act to protect Americans from the harm caused by state AGs who have weaponized their legal authority against the transgender community. It is only a matter of time before AGs expand the use of the surveillance tools to target others seeking necessary medical care, like abortion care.

In the wake of the *Dobbs* decision, Congressional Democrats urged HHS to update the HIPAA privacy rule to protect Americans' health records from warrantless law enforcement disclosures. In April of last year, HHS announced a draft update to the HIPAA Privacy Rule, which offered some modest, but insufficient protections for reproductive health data by creating a hard-to-enforce certification structure and not taking into account secondary use of medical records or data. Forty-seven members of Congress called on HHS to go further to require a warrant for Americans' medical record releases to law enforcement and to close these other policy gaps. In December, Chairman Wyden along with Representatives Jayapal and Jacobs sent a letter to HHS detailing the findings of an oversight inquiry into the inadequate pharmacy privacy practices at eight major pharmacy chains. None of the surveyed pharmacies require a warrant prior to sharing prescription records with law enforcement, and some pharmacies do not even require legal professionals to review medical record demands. Further, only one pharmacy requires patient notification following law enforcement disclosures.

Until HHS acts to raise the bar on patient privacy, patients will look to their providers and their affiliated hospitals to ensure that their intimate health information is safe. The ethical foundations of privacy laws, such as HIPAA, mirror the same fundamental principles of healthcare professionalism and the doctor-patient relationship, like trust, respect for autonomy, and fidelity. As a leader and a convener of hospitals, your hospital association is best positioned to make sure its members are appropriately safeguarding patient privacy by establishing and disseminating best practices for medical privacy to safeguard against future bad faith investigations.

Hospitals should proactively protect sensitive, patient-identifiable information. The significant increase in debilitating cyberattacks against hospitals and other parts of the healthcare ecosystem, such as the recent Change Healthcare fiasco, highlights the need for sound data security practices. As the National Institute for Standards and Technology (NIST) has noted, "[t]he likelihood of harm caused by a breach involving [Personal Identifiable Information (PII)] is greatly reduced if an organization minimizes the amount of PII it uses, collects, and stores." **Hospitals should consider implementing data minimization and destruction policies** that protect patients from foreseeable harm caused by health data breaches. Further, **hospital administrators should establish policies and procedures to respond to legal demands**, including from law enforcement agencies, so that hospitals are equipped to respond in a manner that safeguards patient privacy.

There are clear best practices to protect patient privacy that hospitals should implement once they receive legal demands. **Hospitals should insist on a higher legal standard in response to demands by law enforcement for unredacted patient medical records**, as WashU and SCH did, when they have a good-faith legal rationale for doing so. This mirrors the approach taken by technology companies to protect the privacy of their customers' communications. In 2010, after a federal court of appeals held that Americans have a reasonable expectation of privacy in their emails, and that the 1986 law permitting disclosures of email pursuant to a subpoena was unconstitutional, all major free email providers started requiring a warrant prior to disclosing such data – nationwide. By applying a single appeals court decision across the country, the email provider industry acted on its own to respond to the courts and successfully raised the threshold for the legal process required to access Americans' emails.

Just as SCH refused to comply with the Texas AG's request for its medical records, **hospitals should closely review whether an out-of-state AG has any legal authority to demand medical records beyond its state border.** Because out-of-state demands raise troubling legal concerns, hospitals should pursue judicial review of these demands to ensure they comply with state and federal law and the Constitution, including heightened scrutiny of the demand under a state's shield law, if applicable, that would demand a higher standard of protection for patient records. A similar system already exists for requests from foreign governments: these demands are routed to the Department of Justice for verification and compliance with the law. Likewise, **hospitals should consider referring out-of-state demands to their state AG's office when their state AG has a demonstrated track record of protecting patient privacy**, so that they may work in partnership to evaluate the claim. This practice will also minimize the resource strain that some hospitals may face in pushing back against these types of demands.

In the event of patient record disclosures, absent a non-disclosure or "gag" order issued by a judge, **hospitals should proactively and promptly notify patients about record disclosures to law enforcement entities and AGs**. Further, all **hospitals should require law enforcement to provide specific and detailed supporting information for having satisfied the three-part test for receiving identifiable patient information, prior to sharing any patients' medical information.** Hospitals should refuse to hand over medical information in response to demands that merely rephrase the three-part test in the affirmative.

We are pursuing an all-of-the-above effort to shore-up the health privacy of Americans: we're conducting oversight, we're pushing HHS to improve privacy regulations, and now we're asking hospitals and their associations to do their part to protect patients' privacy rights. Your hospital association has the know-how to establish and spread best practices throughout the healthcare industry. Your position – with open communication channels to hospitals throughout the nation – and an established role as a trusted guide to your members, makes your hospital association the logical stakeholder to take up this task. We urge you this calendar year to establish best practices for patient privacy, schedule a roundtable where relevant stakeholders, including

policymakers, can develop best practices, and create a resource toolkit to assist hospitals in pushing back against invasive medical record requests.

Our ultimate goal is to prepare hospitals to use the levers already at their disposal, through HIPAA, to better safeguard the privacy and dignity of trans patients. We look forward to working with you on this important issue.

Sincerely,

Ron Wyden
United States Senator

Bernard Sanders
United States Senator

Sara Jacobs
Member of Congress

Tammy Baldwin
United States Senator

Pramila Jayapal
Member of Congress

Mazie K. Hirono
United States Senator

Mark Pocan
Member of Congress

Jeffrey A. Merkley
United States Senator

Mark Takano
Member of Congress

Sheldon Whitehouse
United States Senator

Elizabeth Warren
United States Senator

Martin Heinrich
United States Senator

Chris Van Hollen
United States Senator

Alex Padilla
United States Senator

Becca Balint
Member of Congress

Robert Garcia
Member of Congress

Rosa L. DeLauro
Member of Congress

James P. McGovern
Member of Congress

Alexandria Ocasio-Cortez
Member of Congress

Brian Schatz
United States Senator

Adam B. Schiff
Member of Congress

Edward J. Markey
United States Senator

Maxwell Alejandro Frost
Member of Congress

Peter Welch
United States Senator

Zoe Lofgren
Member of Congress

Barbara Lee
Member of Congress

Rashida Tlaib
Member of Congress

Anna G. Eshoo
Member of Congress

Summer Lee
Member of Congress

Ayanna Pressley
Member of Congress

Suzanne Bonamici
Member of Congress

Val Hoyle
Member of Congress

Eleanor Holmes Norton
Member of Congress

Cori Bush
Member of Congress

Sylvia R. Garcia
Member of Congress

Raúl M. Grijalva
Member of Congress

Andrea Salinas
Member of Congress

Jasmine Crockett
Member of Congress

Nikema Williams
Member of Congress

Jared Huffman
Member of Congress

Valerie P. Foushee
Member of Congress

Stephen F. Lynch
Member of Congress

Ted W. Lieu
Member of Congress