



GENERAL COMMITTEE MEETING

Thursday, April 12, 2018
3:00 PM to 4:00 PM

Healthcare Leadership Council
750 9th Street, NW, Suite 500 Washington, D.C. 20001

Conference line: (857) 232-0157, 30-40-73#

- 1. Welcome and introductions**
- 2. Guest Speaker: Carson Martinez, Future Privacy Forum** **Attachment 1**
- 3. 42 C.F.R. Part 2 Update**
 - a. 42 CFR Part 2 letter to MACPAC** **Attachment 2**
- 4. Data Clearinghouse Letters** **Attachments 3,4,5**
- 5. OCR RFI Update**
- 6. NH ISAC – HSCC – Task Groups** **Attachments 6,7,8**
- 7. ONC Guide to Getting and Using your Health Records** **Attachment 9**
- 8. Health Datapalooza**
- 9. Additional articles on HIPAA and Privacy** **Attachments 10 - 15**

Carson Martinez

Carson is a Health Policy Fellow at the Future Privacy Forum. She works on issues surrounding health data, particularly where it is not covered by HIPAA. These non-HIPAA health data issues include consumer-facing genetics companies, wearables, medical “big data” and medical device surveillance. Carson also assists with the operation of the Genetics Working Group.

Carson was previously an Intern at Intel with the Government and Policy Group, working on health, technology, and policy. Before joining Intel, She was as an intern for the International Neuroethics Society, and a Research Assistant for both Data-Pop Alliance and New York University.

Carson graduated from Duke University with a Master’s Degree in Bioethics and Science Policy with a concentration in Technology and Data Policy. Carson earned her Bachelor’s Degree in Neuroscience with minors in Philosophy and Psychology from New York University.



March 29, 2018

Penny Thompson, MPA
Medicaid and CHIP Payment and Access Commission
MACPAC
1800 M St. NW Suite 650 South
Washington, D.C. 20036

Dear Ms. Thompson:

The Healthcare Leadership Council (HLC) is writing to express our support for the MACPAC recommendations for Substance Use Disorder Confidentiality Regulations and Care Integration in Medicaid. HLC believes these recommendations will help the U.S. Department of Health and Human Services (HHS) clarify key components, and coordinate education and technical assistance within 42 CFR Part 2 (Part 2) across relevant agencies. HLC agrees with the commission's finding that Part 2 in its current form remains a barrier to integrating behavioral healthcare, and the need to enable the appropriate exchange of necessary information among medical professionals who are treating individuals with substance use disorders, including opioid abuse, is crucial.

We commend the U.S. Substance Abuse and Mental Health Service Administration's (SAMHSA's) recent letter to Representatives Mullin (R-OK) and Blumenauer (D-OR) stating they agree that a patient's full medical record should be shared with all healthcare providers for the purposes of treatment. This letter highlights SAMHSA's interest but regulatory limits to amend and align Part 2 with the Health Insurance Portability and Accountability Act (HIPAA) to integrate behavioral and physical healthcare, which would help increase access to relevant health information among patients, payers, and providers, while concurrently protecting patient privacy.

HLC is a coalition of chief executives from all disciplines within American healthcare. It is the exclusive forum for the nation's healthcare leaders to jointly develop policies, plans, and programs to achieve their vision of a 21st century health system that makes affordable, high-quality care accessible to all Americans. Members of HLC – hospitals, academic health centers, health plans, pharmaceutical companies, medical device manufacturers, laboratories, biotech firms, health product distributors, pharmacies, post-acute care providers, and information technology companies – advocate for measures to increase the quality and efficiency of healthcare through a patient-centered approach. Through this diversity, we develop a nuanced perspective on the impact of any legislation or regulation affecting the privacy and security of health consumers. We believe access to timely and accurate patient information

leads to both improvements in quality and safety and the development of new lifesaving and life-enhancing medical interventions.

Current federal regulations governing the confidentiality of drug and alcohol treatment and prevention records Part 2 preclude the Centers for Medicare and Medicaid Services (CMS) from disclosing medical information to healthcare providers for care coordination, including those engaged in accountable care organizations and bundled payment organizations. These regulations currently require complex and multiple patient consents for the use and disclosure of patients' substance use records that go beyond the sufficiently strong patient confidentiality protections that were put in place by HIPAA after the implementation of Part 2.

Electronic health records and value-based payment models such as Accountable Care Organizations (ACOs), Health Information Exchanges (HIEs), Medicaid Health Homes, and related Medicare and Medicaid integrated care programs were designed to create a more holistic, patient-centered approach to healthcare where providers work together to coordinate across their traditional silos and in some cases are held jointly accountable for the quality, outcomes, and cost of that care. Critical to making these new models work for patients is having access to the individuals' health records, including those related to substance use disorders. CMS provides participating providers of Medicare ACO and bundled payment organizations with monthly Medicare Parts A, B and D claims under data use agreements that include criminal penalties for misuse. Yet, due to outdated laws mentioned above, CMS is forced to remove *all* claims where substance use disorder is a primary or secondary diagnosis. Patient safety is also threatened with the potential pharmaceutical contraindications that could occur without access to the full medical record. Without this critical information, providers are prevented from understanding the full extent of their patients' medical needs.

Once again, we commend MACPAC's recent recommendations that the Secretary of HHS direct salient agencies to issue regulatory guidance to clarify Part 2 provisions and provide educational and technical assistance on Part 2. We understand SAMHSA has done as much as possible under its regulatory authority in regards to attempts to modernize the Part 2 Rule.

Thank you for your attention to this important matter. Should you have any questions, please contact Tina Grande at 202.449.3433 or tgrande@hlc.org.

Sincerely,

A handwritten signature in black ink, appearing to read "Mary R. Grealy". The signature is fluid and cursive, with the first name "Mary" being the most prominent.

Mary R. Grealy
President



March 29, 2018

The Honorable Greg Walden
Chairman
Energy and Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
Energy and Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Walden and Ranking Member Pallone:

The Confidentiality Coalition appreciates the opportunity to comment on H.R. 4613, "The Ensuring Patient Access to Healthcare Records Act of 2017."

The Confidentiality Coalition is a broad group of organizations working to ensure that policies are implemented to appropriately balance the protection of confidential health information with the efficient and interoperable systems needed to provide high quality healthcare. Access to timely and accurate patient information leads to both improvements in quality and safety and the development of new lifesaving and life-enhancing medical interventions.

The Confidentiality Coalition is comprised of hospitals, medical teaching colleges, health plans, pharmacies, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacy benefit managers, health information and research organizations, clinical laboratories, and others. Through this diversity, we develop a nuanced perspective on the impact of any legislation or regulation affecting the privacy and security of health consumers.

The Confidentiality Coalition supports the committee's intent to ensure access to patient health data to support medical care and innovative payment models that lower healthcare costs. However, coalition members are concerned that H.R. 4613 would eliminate important privacy protections and patient-centered business practices that are regulated through the Health Insurance Portability and Accountability Act (HIPAA) privacy rule without providing meaningful benefits for patients.

As we read the bill, it would authorize disclosure of protected health information (PHI) beyond today's HIPAA rules without any new protections for this data, and in some circumstances, with weakened protections for this information, as it would permit the use and disclosure of PHI by clearinghouses without patient knowledge of clearinghouse existence and/or clearinghouse data use activity. The coalition has the following concerns about H.R. 4613:

- Some of HIPAA's privacy protections for PHI and individuals would be eliminated under H.R. 4613.
 - The bill would invalidate existing business associate agreements between clearinghouses and healthcare providers, plans and other entities that establish protections for PHI. Further, it would permit clearinghouses to engage in the full

- range of treatment, payment and operations activities even though clearinghouses do not have a relationship with patients.
- If a clearinghouse does not have “direct interaction” with an individual the clearinghouse would not have to follow HIPAA regulations that grant individual rights. And most clearinghouses would not have a direct relationship with an individual.
 - The bill requires clearinghouses to post a website notice of privacy practices, but most patients will not have any direct interaction with the clearinghouse and therefore will have no basis to know that the clearinghouse is using their information or that a notice of privacy practices is available.
- While the bill would grant clearinghouse broad new rights to use and disclose patient data, it would not provide appropriate protections to individuals if the clearinghouse has a security breach.
 - Clearinghouses would have to provide breach notification to affected individuals only in limited situations where they are in “direct interaction” with individuals. Since clearinghouses typically do not perform functions for individuals, the clearinghouses almost never interact with individuals.
 - There is a fallback provision that would require covered entities (with a direct patient relationship) to provide notice, but this would be in situations where the covered entities did nothing wrong at all and where there is no business associate agreement (because of this legislation) to protect the covered entities.
 - The bill also permits clearinghouses to charge fees to patients for their records that could be far higher than the fees set by HIPAA regulations and guidance. Under the bill, clearinghouses may purchase PHI from other clearinghouses, create longitudinal patient records, and then charge fair market value for the longitudinal record.
 - Only clearinghouses would be able to buy and sell PHI amongst each other to prepare record requests.

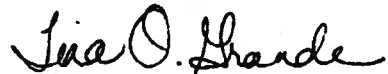
We are also concerned about ambiguities or inconsistent provisions in this bill. There are references to expanding the role of covered entities as well as the role of clearinghouses and genetic information privacy, but the impact of expanding covered entity authority is not well defined.

Lastly, in light of recently announced and/or implemented government initiatives that aim to improve the flow of health data and patient access to health, such as the HHS Office of National Coordinator's Trusted Exchange Framework and Common Agreement (TEFCA); HHS' MyHealthEData Initiative, including Blue Button 2.0; the forthcoming notice of proposed rulemaking on information blocking; as well as the ongoing work of Qualified Entities under CMS' Qualified Entity Certification Program, we urge Congress to allow these initiatives to develop and mature, rather than substantially re-write HIPAA, which has served patients well since its implementation.

For these reasons, members of the Confidentiality Coalition oppose H.R. 4613. While we applaud the intent of H.R. 4613, we respectfully request the committee consider alternative approaches to data that support medical care and improve healthcare payment models. Members of the Confidentiality Coalition stand ready to engage with the committee to examine proposed approaches that will appropriately enable healthcare data flow, protect patient

information and privacy, and are equitable among all stakeholders. Please contact Tina Grande, Senior Vice President for Policy at the Healthcare Leadership Council on behalf of the Confidentiality Coalition at tgrande@hlc.org or at (202) 449-3433 if there are any comments or questions about the comments in this letter.

Sincerely,

A handwritten signature in black ink that reads "Tina O. Grande". The signature is written in a cursive style with a large, looped initial "T".

Tina Grande
Healthcare Leadership Council on behalf of the Confidentiality Coalition



March 29, 2018

The Honorable Kevin Brady
Chairman
Ways and Means Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Richard Neal
Ranking Member
Ways and Means Committee
U.S. House of Representatives
Washington, D.C 20515

Dear Chairman Brady and Ranking Member Neal:

The Confidentiality Coalition appreciates the opportunity to comment on H.R. 4613, "The Ensuring Patient Access to Healthcare Records Act of 2017."

The Confidentiality Coalition is a broad group of organizations working to ensure that policies are implemented to appropriately balance the protection of confidential health information with the efficient and interoperable systems needed to provide high quality healthcare. Access to timely and accurate patient information leads to both improvements in quality and safety and the development of new lifesaving and life-enhancing medical interventions.

The Confidentiality Coalition is comprised of hospitals, medical teaching colleges, health plans, pharmacies, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacy benefit managers, health information and research organizations, clinical laboratories, and others. Through this diversity, we develop a nuanced perspective on the impact of any legislation or regulation affecting the privacy and security of health consumers.

The Confidentiality Coalition supports the committee's intent to ensure access to patient health data to support medical care and innovative payment models that lower healthcare costs. However, coalition members are concerned that H.R. 4613 would eliminate important privacy protections and patient-centered business practices that are regulated through the Health Insurance Portability and Accountability Act (HIPAA) privacy rule without providing meaningful benefits for patients.

As we read the bill, it would authorize disclosure of PHI beyond today's HIPAA rules without any new protections for this data, and in some circumstances, with weakened protections for this information, as it would permit the use and disclosure of protected health information (PHI) by clearinghouses without patient knowledge of clearinghouse existence and/or clearinghouse data use activity. The coalition has the following concerns about H.R. 4613:

- Some of HIPAA's privacy protections for PHI and individuals would be eliminated under H.R. 4613.
 - The bill would invalidate existing business associate agreements between clearinghouses and healthcare providers, plans and other entities that establish protections for PHI. Further, it would permit clearinghouses to engage in the full

- range of treatment, payment and operations activities even though clearinghouses do not have a relationship with patients.
 - If a clearinghouse does not have “direct interaction” with an individual the clearinghouse would not have to follow HIPAA regulations that grant individual rights. And most clearinghouses would not have a direct relationship with an individual as they do with their providers and health plans.
 - The bill requires clearinghouses to post a website notice of privacy practices, but most patients will not have any direct interaction with the clearinghouse and therefore will have no basis to know that the clearinghouse is using their information or that a notice of privacy practices is available.
- While the bill would grant clearinghouse broad new rights to use and disclose patient data, it would not provide appropriate protections to individuals if the clearinghouse has a security breach.
 - Clearinghouses would have to provide breach notification to affected individuals only in limited situations where they are in “direct interaction” with individuals. Since clearinghouses typically do not perform functions for individuals, the clearinghouses almost never interact with individuals.
 - There is a fallback provision that would require covered entities (with a direct patient relationship) to provide notice, but this would be in situations where the covered entities did nothing wrong at all and where there is no business associate agreement (because of this legislation) to protect the covered entities.
- The bill also permits clearinghouses to charge fees to patients for their records that could be far higher than the fees set by HIPAA regulations and guidance. Under the bill, clearinghouses may purchase PHI from other clearinghouses, create longitudinal patient records, and then charge fair market value for the longitudinal record.
 - Only clearinghouses would be able to buy and sell PHI amongst each other to prepare record requests.

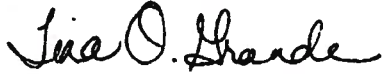
We are also concerned about ambiguities or inconsistent provisions in this bill. There are references to expanding the role of covered entities as well as the role of clearinghouses and genetic information privacy, but the impact of expanding covered entity authority is not well defined.

Lastly, in light of recently announced and/or implemented government initiatives that aim to improve the flow of health data and patient access to health, such as the HHS Office of National Coordinator’s Trusted Exchange Framework and Common Agreement (TEFCA); HHS’ MyHealthEData Initiative, including Blue Button 2.0; the forthcoming notice of proposed rulemaking on information blocking; as well as the ongoing work of Qualified Entities under CMS’ Qualified Entity Certification Program, we urge Congress to allow these initiatives to develop and mature, rather than substantially re-write HIPAA, which has served patients well since its implementation.

For these reasons, members of the Confidentiality Coalition oppose H.R. 4613. While we applaud the intent of H.R. 4613, we respectfully request the committee consider new approaches to data that support medical care and improve healthcare payment models. Members of the Confidentiality Coalition stand ready to engage with the committee to examine proposed approaches that will appropriately enable healthcare data flow, protect patient

information and privacy, and are equitable among all stakeholders. Please contact Tina Grande, Senior Vice President for Policy at the Healthcare Leadership Council on behalf of the Confidentiality Coalition at tgrande@hlc.org or at (202) 449-3433 if there are any comments or questions about the comments in this letter.

Sincerely,

A handwritten signature in black ink that reads "Tina O. Grande". The signature is written in a cursive style with a large, prominent "T" and "G".

Tina Grande
Healthcare Leadership Council on behalf of the Confidentiality Coalition



March 29, 2018

The Honorable Lamar Alexander
 Chairman
 U.S. Senate Committee on Health, Education,
 Labor, and Pensions
 Washington, D.C. 20510

The Honorable Patty Murray
 Ranking Member
 U.S. Senate Committee on Health, Education,
 Labor, and Pensions
 Washington, D.C. 20510

Dear Chairman Alexander and Ranking Member Murray:

The Confidentiality Coalition appreciates the opportunity to comment on H.R. 4613, "The Ensuring Patient Access to Healthcare Records Act of 2017."

The Confidentiality Coalition is a broad group of organizations working to ensure that policies are implemented to appropriately balance the protection of confidential health information with the efficient and interoperable systems needed to provide high quality healthcare. Access to timely and accurate patient information leads to both improvements in quality and safety and the development of new lifesaving and life-enhancing medical interventions.

The Confidentiality Coalition is comprised of hospitals, medical teaching colleges, health plans, pharmacies, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacy benefit managers, health information and research organizations, clinical laboratories, and others. Through this diversity, we develop a nuanced perspective on the impact of any legislation or regulation affecting the privacy and security of health consumers.

The Confidentiality Coalition supports the House Energy and Commerce and Ways and Means Committees' intent to ensure access to patient health data to support medical care and innovative payment models that lower healthcare costs. However, coalition members are concerned that H.R. 4613 would eliminate important privacy protections and patient-centered business practices that are regulated through the Health Insurance Portability and Accountability Act (HIPAA) privacy rule without providing meaningful benefits for patients.

As we read the bill, it would authorize disclosure of protected health information (PHI) beyond today's HIPAA rules without any new protections for this data, and in some circumstances, with weakened protections for this information, as it would permit the use and disclosure of protected PHI by clearinghouses without patient knowledge of clearinghouse existence and/or clearinghouse data use activity. The coalition has the following concerns about H.R. 4613:

- Some of HIPAA's privacy protections for PHI and individuals would be eliminated under H.R. 4613.
 - The bill would invalidate existing business associate agreements between clearinghouses and healthcare providers, plans and other entities that establish protections for PHI. Further, it would permit clearinghouses to engage in the full range of treatment, payment and operations activities even though clearinghouses do not have a relationship with patients.

- If a clearinghouse does not have “direct interaction” with an individual the clearinghouse would not have to follow HIPAA regulations that grant individual rights. And most clearinghouses would not have a direct relationship with an individual.
- The bill requires clearinghouses to post a website notice of privacy practices, but most patients will not have any direct interaction with the clearinghouse and therefore will have no basis to know that the clearinghouse is using their information or that a notice of privacy practices is available.
- While the bill would grant clearinghouse broad new rights to use and disclose patient data, it would not provide appropriate protections to individuals if the clearinghouse has a security breach.
 - Clearinghouses would have to provide breach notification to affected individuals only in limited situations where they are in “direct interaction” with individuals. Since clearinghouses typically do not perform functions for individuals, the clearinghouses almost never interact with individuals.
 - There is a fallback provision that would require covered entities (with a direct patient relationship) to provide notice, but this would be in situations where the covered entities did nothing wrong at all and where there is no business associate agreement (because of this legislation) to protect the covered entities.
- The bill also permits clearinghouses to charge fees to patients for their records that could be far higher than the fees set by HIPAA regulations and guidance. Under the bill, clearinghouses may purchase PHI from other clearinghouses, create longitudinal patient records, and then charge fair market value for the longitudinal record.
 - Only clearinghouses would be able to buy and sell PHI amongst each other to prepare record requests.

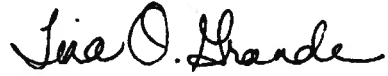
We are also concerned about ambiguities or inconsistent provisions in this bill. There are references to expanding the role of covered entities as well as the role of clearinghouses and genetic information privacy, but the impact of expanding covered entity authority is not well defined.

Lastly, in light of recently announced and/or implemented government initiatives that aim to improve the flow of health data and patient access to health, such as the HHS Office of National Coordinator’s Trusted Exchange Framework and Common Agreement (TEFCA); HHS’ MyHealthEData Initiative, including Blue Button 2.0; the forthcoming notice of proposed rulemaking on information blocking; as well as the ongoing work of Qualified Entities under CMS’ Qualified Entity Certification Program, we urge Congress to allow these initiatives to develop and mature, rather than substantially re-write HIPAA, which has served patients well since its implementation.

For these reasons, members of the Confidentiality Coalition oppose H.R. 4613. While we applaud the intent of H.R. 4613, we respectfully request the Senate HELP Committee consider alternative approaches to data that support medical care and improve healthcare payment models. Members of the Confidentiality Coalition stand ready to engage with the committee to examine proposed approaches that will appropriately enable healthcare data flow, protect patient information and privacy, and are equitable among all stakeholders. Please contact Tina Grande, Senior Vice President for Policy at the Healthcare Leadership Council on behalf of the

Confidentiality Coalition at tgrande@hlc.org or at (202) 449-3433 if there are any comments or questions about the comments in this letter.

Sincerely,

A handwritten signature in black ink that reads "Tina O. Grande". The signature is written in a cursive style with a large, looped initial "T".

Tina Grande
Healthcare Leadership Council on behalf of the Confidentiality Coalition



Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTHCARE SECTOR COORDINATING COUNCIL

What Is It?

- The cross-sector coordinating body representing one of 16 critical infrastructure sectors identified in Presidential Executive Order ([PPD-21](#))
- A trust-community partnership convening companies, non-profits and industry associations across six subsectors with HHS, DHS, law enforcement, and intelligence community
- ***Mission: to identify cyber and physical risks to the security and resiliency of the sector, and develop planning guidance in a 3-year [Sector Specific Plan](#) and implementing task groups for mitigating those risks***
- In meeting with government, it is the “Healthcare & Public Health SCC (HPH SCC)”
- Focused on longer-term critical infrastructure policy and strategy, complementing the operational National Health Information Sharing and Analysis Center, which serves as the sector’s tactical watch, warning, incident response, forensics, and best practices hub for intra-sector and government information sharing



Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Information Sharing TG (Todd)

- Members: Al Roeder; Bruce James; Connie Barrera; Ed Brennan; Greg Garcia; Lee Barrett; Michael Pry; Michael Vermilye; Nick Boukas; Nickol Todd; Tarik Rahmanovic; Terry Donat; Gary Fagan (*ADDITIONAL PARTICIPANTS WELCOMED*)
- Deliverables: TBD (See status)
- Task: Analyze existing and encourage new information-sharing activities regarding threat information, security incidents including exploits, breaches, and general cybersecurity information between government and private sector; develop or leverage existing timely, actionable incident management and cybersecurity alerts/guidance/best practices/educational materials, etc. for different types of audiences
- Anticipated Products: ISAO cyber security awareness within the HPH sector and support sector stakeholders to take action in response to CTI shared
- Meeting Frequency: Every 2nd Monday of the month @ 10:30am ET.
- Status:
- Review of HCIC Task Force recommendations on information sharing completed; most critical identified as:
 - **Action Item 6.1.1** - HHS / Information Sharing and Analysis Organizations (ISAOs) should streamline and consolidate information sharing data on threats whenever practical for easier consumer adoption
 - **Action Item 6.3.3** - HHS, DHS NCCIC, and law enforcement should maintain unified and dedicated channels during steady state and response efforts to provide SME support, leveraging existing relationships and facilitate targeted dissemination ...
 - **Action Item 6.2.2** - HHS / fed partners should ensure intelligence reports and threat information is consolidated and given additional context as distributed industry
- Comments on draft *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* are due February 12, 2018



Future Gazing TG (Jarrett/Katona)

- Members: Mark Jarrett, MD; Peter Katona, MD; Brian Quinn; Jay Kirkpatrick; Sanjeev Sah; Kelly Aldrich
- Deliverables: TBD
- Task: Develop an ongoing dialogue on how to incorporate new technology into healthcare and public health practice without compromising patient safety or access by individuals to their data as required by law
- Anticipated Products: Best practices submitted by members to include specific medical and IOT devices to be shared via a white paper or web posting
- Meeting Frequency: Monthly
- Next Meeting:
- Status:



Information Sharing TG (Todd)

- Members: Al Roeder; Bruce James; Connie Barrera; Ed Brennan; Greg Garcia; Lee Barrett; Michael Pry; Michael Vermilye; Nick Boukas; Nickol Todd; Tarik Rahmanovic; Terry Donat; Gary Fagan (*ADDITIONAL PARTICIPANTS WELCOMED*)
- Deliverables: TBD (See status)
- Task: Analyze existing and encourage new information-sharing activities regarding threat information, security incidents including exploits, breaches, and general cybersecurity information between government and private sector; develop or leverage existing timely, actionable incident management and cybersecurity alerts/guidance/best practices/educational materials, etc. for different types of audiences
- Anticipated Products: ISAO cyber security awareness within the HPH sector and support sector stakeholders to take action in response to CTI shared
- Meeting Frequency: Every 2nd Monday of the month @ 10:30am ET.
- Status:
- Review of HCIC Task Force recommendations on information sharing completed; most critical identified as:
 - **Action Item 6.1.1** - HHS / Information Sharing and Analysis Organizations (ISAOs) should streamline and consolidate information sharing data on threats whenever practical for easier consumer adoption
 - **Action Item 6.3.3** - HHS, DHS NCCIC, and law enforcement should maintain unified and dedicated channels during steady state and response efforts to provide SME support, leveraging existing relationships and facilitate targeted dissemination ...
 - **Action Item 6.2.2** - HHS / fed partners should ensure intelligence reports and threat information is consolidated and given additional context as distributed industry
- Comments on draft *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* are due February 12, 2018

FOR IMMEDIATE RELEASE
April 4, 2018

Contact: HHS Press Office
202-690-6343
media@hhs.gov

HHS Releases a New Resource to Help Individuals Access and Use Their Health Information

The US Department of Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC) today released the [*ONC Guide to Getting and Using your Health Records*](#), a new online resource for individuals, patients, and caregivers.

This new resource supports both the 21st Century Cures Act goal of empowering patients and improving patients' access to their electronic health information and the recently announced [MyHealthEData initiative](#). The new initiative, led by the White House Office of American Innovation and supported by ONC, empowers patients by giving them control of their healthcare information. Other participants in the effort include the Centers for Medicare & Medicaid Services, National Institutes of Health, and the Department of Veterans Affairs.

"It's important that patients and their caregivers have access to their own health information so they can make decisions about their care and treatments," said Don Rucker, M.D., national coordinator for health information technology. "This guide will help answer some of the questions that patients may have when asking for their health information."

Individuals' ability to access and use their health information electronically is a measure of interoperability and a cornerstone of ONC's efforts to increase patient engagement, improve health outcomes, and advance person-centered health.

In fact, a new [ONC data brief - PDF](#) shows that in 2017, half of Americans reported they were offered access to an online medical record by a provider or insurer. This is up from 42 percent in 2014. Over half of individuals who were offered online access viewed their record with the past year. Eight in 10 of the individuals who viewed their information rated their online medical records as both easy to understand and useful for monitoring their health. These positive perceptions may be attributed to individuals' varied use of online medical records, including viewing test results; managing their health needs with greater convenience; communicating with their health care provider; self-management and treatment decision-making; and contributing information to and correcting errors in their medical record.

However, challenges remain. Almost half of Americans in 2017 who were offered access to an online medical record did not access their record, frequently citing a perceived lack of need as one of the reasons for not accessing their record. Consumers may not understand their right (under the HIPAA Privacy Rule) to access their health information nor realize the benefits of accessing their health information. ONC outlined the challenges patients face in accessing their health information electronically in a [report - PDF](#) released in June 2017.

"The ONC Guide to Getting and Using your Health Records" informs patients and consumers about the value of health information, and provides individuals with clear, actionable advice on how to:

- **Get their health record**, including offering tips through the process of accessing their records electronically,
- **Check their health record** to make sure it is complete, correct, and up-to-date, and
- **Use their electronic health records**, such as sharing their records to better coordinate their care and using apps and other digital technologies to better manage and improve their health.

To view the ONC Guide to Getting, Checking, and Using your Health Records, visit: [HealthIT.gov](https://www.healthit.gov).

Additional information on the HIPAA Privacy Rule is available at: <https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html>

###

The comments were made at a cyberrisk quantification conference hosted by Drexel University's LeBow College of Business in Philadelphia as the Dr. cited data from the U.S. Department of Health and Human Services and the Centers for Medicare & Medicaid Services to compare patient-care metrics at hospitals that have and have not experienced a data breach. Choi argued the proportion of heart attack patients who die within 30 days of being admitted to a hospital increased by 0.23 percent one year after a breach and by 0.36 percent two years after a breach, which represents 2,160 additional patient deaths annually.

Leon Lerman, co-founder and CEO of healthcare cybersecurity specialist Cynerio, said it's difficult to get the medical devices back up and running following a breach with many devices requiring assistance from the manufacturers in order to reset them. He went on to say that disruption doesn't have to be caused directly by the breach or attack but could be caused during the investigation process.

"I think it's fair and logical to say that the more often these breaches occur the more likely there will be an increase in patient mortality rates, as it's very likely that during a breach some sort of service disruption will occur and the doctor will be preoccupied and won't be giving full attention to a patient," Lerman said.

Ultimately, Lerman said, it depends on if the breach or attack is visible to the doctors or not to understand the extent of the correlation of attacks.

Apple's Pact with 13 Health Care Systems Might Actually Disrupt the Industry

Friday, March 23, 2018



By [David Blumenthal, M.D.](#) and [Aneesh Chopra](#)

Published March 23, 2018, in the [Harvard Business Review](#). Re-posted with permission.

[An announcement on January 24](#) didn't get the large amount of attention it deserved: Apple and 13 prominent health systems, including prestigious centers like Johns Hopkins and the University of Pennsylvania, disclosed an agreement that would allow Apple to download onto its various devices the electronic health data of those systems' patients — with patients' permission, of course.

It could herald truly disruptive change in the U.S. health care system. The reason: It could liberate health care data for game-changing new uses, including empowering patients as never before.

Since electronic health records (EHRs) became widespread over the last decade, there has been growing frustration over the inability to make electronic data liquid — to have it follow the patient throughout the health system and to be available for more sophisticated analysis in support of improved patient care and research. [Most efforts](#) to liberate and exchange health data have focused on getting doctors and hospitals to share it with one another. Those efforts continue, but progress has been slow.

Frustration has increased interest in a very different approach to data sharing: Give patients their data, and let them control its destiny. Let them share it with whomever they wish in the course of their own health care journey.

Several technology companies — including Google and Microsoft — tried this in the early 2000s, but their efforts failed. There just wasn't that much electronic health data available at the time, since only a tiny fraction of doctors and hospitals had electronic records. Health systems were reluctant to share what data existed, seeing it as a valuable proprietary asset. The technology for giving outside entities access to electronic records kept by hospitals and doctors was underdeveloped. And EHR vendors were uninterested in promoting such access because the demand was weak and data sharing could spur competition from other vendors.

Those obstacles have now mostly melted away. Electronic health records and digitized health data are now ubiquitous. Various federal incentives and regulations now require providers to share data with other providers and with patients or face significant financial penalties. The Argonaut Project, a voluntary private sector collaborative, has provided guidelines for an open source, standardized application programming interface (API) that provides ready access to data stored in providers' electronic records. Think of APIs as [gateways into electronic data warehouses](#) that now populate the health care landscape. Of note, the federal government now requires all vendors of electronic records to include these open APIs in their products to be federally certified.

A world in which patients have ready access to their own electronic data with the help of facilitators like Apple creates almost unfathomable opportunities to improve health care and health. First, participating patients would no longer be dependent on the bureaucracies of big health systems or on understaffed physician offices to make their own data available for further care. This could improve the quality of services and reduce cost through avoiding duplicative and unnecessary testing.

Second, the liberation of patients' data makes it possible for consumer-oriented third parties to use that data (with patients' permission) to provide new and useful services that help patients manage their own health and make better health care choices. Such consumer-facing applications — if they are

designed to be intuitive, useable, and accurate — have the potential to revolutionize patient-provider interactions and empower consumers in ways never before imagined in the history of medicine. Imagine Alexa- or Siri-style [digital health advisors](#) that can respond to consumer questions based on users' unique health care data and informed by artificial intelligence. Health care could start to function much more like traditional economic markets.

Nevertheless, this vision of the future faces obstacles and uncertainties.

First, large numbers of hospitals and doctors have to follow the lead of the 13 systems that have already jumped on board. There are encouraging signs that many more will join, but ultimately, there needs to be a clear business case for both providers and their IT allies to invest in this new partnership. Perhaps the most compelling would be widespread consumer demand for the service. For that demand to materialize, consumers have to receive something they value in return for giving third parties like Apple access to their data. This means that Apple and its future competitors will have to develop nifty consumer-facing apps that solve consumer health-related problems easily and cheaply. Those apps simply don't exist at the moment.

Second, the opportunities for fraud and abuse in this new world of data access are daunting. Most consumers will want to delegate to third parties the job of accessing, storing, managing, and analyzing their data. Making sure those third parties are trustworthy is critical, and unscrupulous actors will inevitably take advantage of unsophisticated patients. Health data is extremely valuable on illicit markets. And even honest but unsophisticated data stewards can create huge problems if they don't adequately protect patient information. Federal and private sector organizations are trying to develop a voluntary but enforceable code of conduct to govern the behavior of private data stewards. This would be an important first step toward assuring that consumers are not victimized on the way to a brighter health care future.

Third, once new companies start to develop consumer-facing health applications based on patients' own health care data, the quality of those applications could become an important issue. If they offer advice, it needs to be reliable. If they promise a service, they need to deliver. Some applications may fall within the existing regulatory authorities of U.S. federal agencies like the Food and Drug Administration or the Federal Trade Commission. If not,

the question of whether and how to assure that the advice furnished consumers is valid and reliable will certainly arise as a matter of public policy.

These problems notwithstanding, the announcement of this collaboration between leading American providers of health and information technology services likely signals a new era in health and medicine. The partnership and its results will not solve all our health care problems. But they could really shake things up. And that is what the U.S. health system needs.

Putting patient data on phones introduces new privacy and security concerns

Modern Healthcare

By [Rachel Z. Arndt](#) | March 31, 2018

The recent push from both Apple and the CMS to give patients more control of their own health data stands to boost patient engagement, which most in the industry consider a good thing. But moving data outside of the relatively safe confines of an electronic health record adds another layer of risk and vulnerability.

As more parties gain access to the data, more avenues for breaches open up, potentially jeopardizing not just information security but also patient privacy. Bad actors can now target not only EHR systems but also patients' phones, where health data reside.

Those pools of data will only grow larger. Last week, Apple officially launched the next iteration of its Health app, which allows people to pull their electronic health record data onto their iPhones. Thirty-nine health systems have partnered with the tech giant to make their patients' data available. "When you have this data on your phone, you have risks that would traditionally not have existed," said Daniel Farris, chair of the technology practice at Fox Rothschild.

Even Facebook's Mark Zuckerberg can attest that no organization is immune from public—and potentially political—backlash when sensitive consumer data is compromised. Many argue that Facebook's problems with Cambridge Analytica and access to user data should serve as a wake-up call to technology executives who have been entrusted to protect consumer information.

Allowing patients to put data on their phones isn't just a matter of flipping a switch and then walking away. It's first and foremost the patient's responsibility to keep the data secure and private. Health systems and vendors alike are encouraging patients to understand the risks and take precautions. "The patient who downloads this information absolutely must secure their device to protect their own records," said John Kravitz, chief information officer at Danville, Pa.-based Geisinger, one of the first health systems to link its records with Apple's Health app.

But getting the data onto those phones requires security safeguards on the part of the health system and EHR vendor too. Because of those safeguards, the actual movement of the data shouldn't pose too great a security risk, argued Steve Dunkel, chief information security officer at Geisinger.

Just as a patient has to go through authentication to access a patient portal on their phone, they do the same when granting the Health app access to their records. The app then makes a secure connection and receives the data via the FHIR standard.

While security can be built directly into the app, some encouraged using security controls already available on phones. "Patients have requirements for strong passwords, and we can make them more secure by using newer features like Touch ID on the patient's mobile phone," said Janet Campbell, vice president of patient engagement for Epic Systems Corp.

This drive to get patient data into patients' hands comes not only from companies and health systems but also from the federal government. Jared Kushner, senior adviser to President Donald Trump, and CMS Administrator Seema Verma want to increase interoperability and give patients more control of their own data, they announced at the Healthcare Information and Management Systems Society's annual meeting in March.

But the federal government's new zeal for data mobility should be accompanied by a push for security standards, said John Riggi, an FBI veteran who's now senior adviser for cybersecurity and risk at the American Hospital Association. "The issue surrounding apps in particular is that (the Office of the National Coordinator for Health Information Technology) has not promulgated specific security standards," he said.

While some apps, like those made by EHR vendors, abide by HIPAA security and privacy rules by law, once data are on a patient's phone, the patient might unwittingly share them with an app that doesn't have such stringent security and privacy controls. "There should be a measured approach in collaboration with HHS and the ONC and the providers to ensure whatever platform a patient uses to access the EHR has been fully vetted and complies with all HIPAA privacy and security rules," Riggi said.

There's also the threat of malicious apps, which might be able to extract patient health information. Malware of this sort already exists to steal financial and other data, and benevolent apps already share information with advertisers.

"This is not as much a concern when you're dealing with a large, trusted organization such as Apple," Riggi said. Apple requires patients to authenticate the data transfer by logging into their health systems' EHR patient portals. Data then travel straight from the portal into the app, never passing through Apple servers.

Patients can bear some of the responsibility, primarily by ensuring the app is from a trusted vendor. Indeed, information technologists stress the need for education.

"We enthusiastically support the consumer's right to access a copy of their data and to decide how it should be used," said Don Bisbee, senior vice president of clinical and business strategy for Cerner. "But continued education is needed around the potential risks associated with choosing to expose sensitive health data to broader groups than the covered entities where HIPAA protections apply."

Riggi compared the need for security in healthcare apps to the need for security in

financial apps. But financial apps, he pointed out, are entirely controlled by the financial institutions they're related to, whereas health apps aren't necessarily controlled by health systems. "There should be a measured approach with collaboration between HHS and ONC and the providers to ensure whatever platform a patient uses to access the EHR has been fully vetted and complies with all HIPAA privacy and security rules," Riggi said.

The type of data contained in the Health app (and others) complicates how HIPAA would apply, though. The Health app won't just hold protected health information from EHRs. It'll also hold patient-generated data from wearables and other sources—data that aren't considered protected health information but could, in theory, be turned into it.

"The same set of data may be subject to HIPAA or not depending on where it is or who accessed it, and that could create drastically different privacy and security requirements," Farris said.

For example, if a person has data from a wearable on their phone and only that person has accessed the data, then the data aren't considered protected health information. But as soon as that person shares the data with a provider, intending it to be used for healthcare purposes, the data become protected. If that data were breached somehow, it would be considered a HIPAA violation. That, in turn, raises the question of who would be responsible for such a breach. "If there's a failure of security at the phone level, maybe Apple is liable," Farris said. "If there's a failure at the app level, it might be the app maker, and if there's insecure transmission, it might be the EHR vendor."

For instance, if a patient downloads their information to the Health app and then posts it on Twitter, that's not a violation of HIPAA. But if that patient inadvertently lets a third-party app access their information, who's responsible? Even though the data may still be secure, they're no longer private—and that's concerning, Farris said.

"You can't have privacy without security, but you can have security without privacy," he added.

March 27, 2018

Congress Grappling With Privacy Questions in Opioid Crisis

From [Health Care on Bloomberg Law](#)

Stay ahead of developments in federal and state health care law, regulation and transactions with timely, expert news and analysis.

By [Alex Ruoff](#)

Changes to federal health privacy rules restricting doctors' access to drug treatment records could play a major role in Congress's response to the opioid epidemic in the coming months.

Lawmakers recently passed a measure meant to help better flag for doctors when a person they're treating has a history of substance use. Jessie's Law was created for a woman who died from an overdose after being given a prescription for oxycodone despite telling her doctor she was recovering from an opioid addiction.

But the bill doesn't solve the problem at the heart of the issue: Hospitals and doctors often can't keep substance use records with the rest of a patient's health history, leaving them without crucial information. A coalition of behavioral health and information management groups wants to change that by aligning federal health privacy rules so all health data must be treated the same.

"By aligning, we can get better coordination for patients, avert risk, and give them better care," Duanne Pearson, senior director for federal affairs for Premier Inc., an alliance of thousands of hospitals and physicians, told Bloomberg Law.

Some substance abuse treatment providers, however, worry relaxing federal privacy rules could discourage some people from seeking drug addiction treatment out of fear their records will end up the wrong hands.

Substance abuse treatment records are protected by a 40-year-old statute commonly referred to as Part 2, which generally requires specific, written consent by the patient in order to be shared among doctors and hospitals. Most of a person's other health data can be shared among the health-care providers who treat them for treatment, payment, or operations purposes.

To comply with these stricter rules most hospitals or doctors' offices that keep substance use treatment data simply separate the files, with the result that drug treatment data are often not shared among doctors, Lauren Riplinger, senior director of federal relations for the American Health Information Management Association, told

Bloomberg Law. Electronic records typically can't separate the data either, so most drug treatment records are often left on paper while the rest of a person's health history is digitized.

This means doctors sometimes don't know if their patients have a history of drug or alcohol abuse, even if they've gotten treatment, and hospitals and doctors in integrated care models are missing crucial information, Riplinger said. This separation of the data also means some drug treatment centers are struggling to participate in some integrated care models, for which they have to share their patient data.

It also means researchers generally don't have access to substance use disorder records. The Centers for Medicare & Medicaid Services didn't include roughly 4.5 percent of inpatient Medicare claims and 8 percent of Medicaid claims in key research files because they contained some substance use disorder diagnoses, according to a [2015 study published](#) in the New England Journal of Medicine.

AHIMA is part of a group of more than 30 health-care organizations including the American Hospital Association and the Blue Cross Blue Shield Association, known as the Partnership to Amend 42 CFR Part 2, looking to alter federal privacy rules.

Lawmakers appear eager to tackle the problems around the opioid epidemic, which contributed to 116 deaths each day in 2016, but wary of overhauling federal privacy rules.

What Could Change

The House's champion to alter Part 2 rules, Rep. Tim Murphy (R-Pa.), left Congress late last year after a scandal. His proposal to alter federal privacy laws has been taken up by Reps. Markwayne Mullin (R-Okla.) and Earl Blumenauer (D-Ore.), who have since limited the changes Murphy has proposed.

House lawmakers are considering Mullin's [bill](#) to allow doctors and hospitals to share substance abuse records for treatment purposes, but not for payment or other purposes. This limiting of the bill to just treatment purposes was meant to ease the concern of some lawmakers, Pearson said.

However, Reps. Frank Pallone Jr. (D-N.J.) and Gene Green (D-Texas) still voiced concern the legislation would relax federal privacy laws too much during a recent House Energy and Commerce Committee hearing on the opioid crisis.

Advocates are now weighing if they can return the bill to its original form, Pearson said. The House is expected to take up opioids legislation by Memorial Day, he said.

Hospital groups have warned the limitation might not make a difference in sharing substance use disorder records because of the difficulty in separating treatment and payment purposes.

America's Essential Hospitals, in a [letter](#) to the House Energy and Commerce Committee ahead of a March 22 hearing on the opioid crisis, warned this would mean doctors couldn't share treatment data for care coordination programs or for prescription drug monitoring programs.

To contact the reporter on this story: Alex Ruoff in Washington
ataruoff@bloomberglaw.com

To contact the editor responsible for this story: Brian Broderick
atbroderick@bloomberglaw.com

Copyright © 2018 The Bureau of National Affairs, Inc.

AMA Official Suggests Alternative To HIPAA Regulations To Mitigate Physicians' Cyber Risks

Inside Health Policy

April 03, 2018

The American Medical Association is urging HHS to put out a policy that would encourage physicians to embrace a framework for managing cybersecurity risks in exchange for the government agreeing not to conduct surprise audits under the Health Insurance Portability and Accountability Act, which governs the handling and use of medical records and personal patient information.

The AMA proposal is based on a survey issued by the group late last year that found most physicians saw HIPAA requirements as inadequate for mitigating the risk of a cyber attack and view securing data as key to patient treatment and safety.

The HHS Office for Civil Rights, which enforces HIPAA requirements, "should accept implementation of a cybersecurity framework as 'reasonable and appropriate' under the law," said AMA's Laura Hoffman at the HIPAA Summit in Arlington, VA last Wednesday.

Hoffman, who is assistant director of federal affairs for AMA, told *Inside Cybersecurity* that the group has outlined its proposed policy alternative to ORC officials, whom she said expressed some interest.

"We'll continue to press for it," she said. Hoffman, in her remarks to the health industry and government officials at the conference, stressed physicians can be "incentivized" to conduct a cybersecurity risk assessment because it ranks high for them in delivering patient care according to the AMA survey.

She said a "how-to guide" for use of a cybersecurity framework ranked high among physicians when asked what they need to assess security risks.

A vast majority of physicians, 83 percent, value conducting a security risk assessment "but said HIPAA is not enough to meet their cybersecurity needs," according to Hoffman. Also, 70 percent of physicians said they would pay someone to implement a cybersecurity framework "if they would not be randomly audited by HIPAA."

She said most physicians rely heavily on vendors and IT service providers for training and assurances about data privacy and security, while 83 percent of doctors said it is important to share electronic health records to improve care but are concerned how to do it securely.

Hoffman called for changes in statute to provide a safe harbor for sharing services and technologies among healthcare providers, an issue AMA has raised with congressional staff, she told *Inside Cybersecurity*.

In her remarks, Hoffman said AMA's proposals echo recommendations laid out by the HHS cybersecurity task force, which issued a report last summer under a congressional mandate. Hoffman said AMA is advocating the use of any number of widely recognized cyber frameworks such as the one issued by the National Institute of Standards and Technology -- which all federal agencies are required to use -- or the recently revised framework by the Health Information Trust Alliance, or HITRUST.

Her call for a regulatory alternative was also echoed by other speakers at the event, who highlighted the emerging cyber risks for the health sector and the struggle of policymakers to adapt the current HIPAA regulatory structure to meet these evolving threats.

“Either voluntarily move toward HIPAA” to address cybersecurity “or there will be a bigger [regulatory] regime” to address these new risks,” said former HHS OCR Richard Campanelli in remarks preceding Hoffman's presentation. -- *Rick Weber* (rweber@iwpnnews.com)

Daily News

HHS Secretary Urged To Resolve Cyber Center Dispute As Health Sector Faces Increased Threats

Inside Health Policy

March 29, 2018

HHS Secretary Alex Azar is being pressed to weigh in on a dispute over alleged mismanagement of the department's recently established cyber-threat sharing center, which is undergoing a restructuring that a leading HHS cybersecurity official says could undermine the department's ability to assist the health sector in anticipating and responding to cyber attacks.

The dispute over the Health Cybersecurity and Communications Integration Center stems from anonymous allegations of corruption last year that led HHS CISO Chris Wlaschin to place HCCIC official Leo Scanlon on administrative leave and to remove Maggie Amato as head of the HCCIC last September, pending a review of the cyber center, which is intended to share threat intelligence with healthcare providers, hospitals and drug and device manufacturers.

"Mr. Scanlon is your Deputy Cybersecurity Information Officer (DCISO) and HHS Senior Advisor for HPH Cybersecurity, and Ms. Amato was constructively terminated from her position as your Director of the Healthcare Cybersecurity Communications and Integration Center (HCCIC)," writes a lawyer for Scanlon in a letter to Azar.

"I am writing to call your attention to significant irregularities and possible violations of law carried out by your agency in the treatment of these employees," asserts the lawyer, I. Charles McCullough, in a March 12 letter seeking an in-person meeting with the HHS secretary.

Scanlon has told *Inside Cybersecurity* that Azar has not responded to his request for a meeting and for clarification on the status of an alleged Office of Inspector General investigation of the HCCIC.

The HHS press office did not immediately respond to a request for comment.

"Mr. Wlaschin has stated that my clients were removed from their positions in order to protect an ongoing OIG investigation," states the letter to Azar. "You can, therefore, imagine the shock and surprise of my clients when they were both recently advised, unequivocally and categorically, by senior investigators from the HHS OIG, that neither of them are currently or were at any time in the past under investigation by the OIG," writes lawyer McCullough.

Scanlon and Amato vehemently deny any wrongdoing in setting up and operating the HCCIC, which was credited by lawmakers and others for having mitigated the potential impact in the U.S. of a global

ransomware attack in May 2017 known as WannaCry, which temporarily took out a significant portion of the United Kingdom's public health system.

An HHS OIG spokesperson said the office has a general practice of neither confirming nor denying the existence of an investigation being conducted. "However, because information has come to light that suggests that the OIG was conducting an investigation involving the Healthcare Cybersecurity and Communications Integration Center (HCCIC), we are willing to acknowledge that an OIG investigation involving HCCIC is/was ongoing," the spokesperson said in an email. "We are not at liberty to provide any further details at this time."

The dispute and leadership shakeup at the HCCIC has attracted the attention of Congress. Leaders of House Energy and Commerce Committee sent a bipartisan letter to HHS last November seeking documentation on the operations of the HCCIC.

"The committee is still reviewing the situation and, therefore, cannot provide any information at this time. If there are any updates we can share publicly, we will let you know," said a congressional source in response to a question about a Nov. 28, 2017 deadline for HHS to answer the committee letter.

"Given how critical health care cybersecurity is to the nation and the apparently central role of the new HCCIC in the Department's response to WannaCry, these recent and abrupt changes raise a number of questions about HHS and its commitment to providing effective leadership to the sector," states the Nov. 14, 2017, letter signed by Energy and Commerce Chairman Greg Walden (R-OR) and ranking member Frank Pallone (D-NJ).

HCCIC restructuring

HHS officials have announced intentions to restructure and rebrand the HCCIC, a move that is expected to defer sharing of cyber-threat information to the Department of Homeland Security's National Cybersecurity and Communications Center, which distributes cyber-threat indicators across all sectors of critical infrastructure -- from power plants to financial services -- and predates the HCCIC by nearly 10 years. The anticipated HCCIC restructuring also is expected to shift operations to the HHS' Computer Security Incident Response Center in Atlanta, according to sources.

In a joint interview with *Inside Cybersecurity*, Scanlon and Amato raised concerns that a shift in operations to emphasize the CSIRC would be inward looking for the department in addressing cyber risks, rather than reaching out to the health sector which is widely seen as a prime target for hackers.

"I don't think anything has happened," Amato said in asserting how efforts to broaden industry outreach in the wake of the WannaCry attack were derailed when she and Scanlon were temporarily suspended of their HCCIC duties last September. Amato has since left the government.

Scanlon and Amato noted that CSIRC operates under the HHS assistant secretary for administration, while the department's efforts in dealing with public health threats, such as pandemics as well as potential cyber attacks, falls to the Office of the Assistant Secretary for Preparedness and Response.

"We were trying to leverage that work," Amato said, in describing how the HCCIC was intended to be the out-facing source for cyber-threat information to healthcare providers both large and small.

HHS officials have offered scant details on the upcoming HCCIC restructuring, but industry sources who have been following the process say they expect it to be operational very soon.

Wlaschin outlined the department's objectives for the HCCIC as part of the Health Threat Operations Center, in remarks at the Health Information and Management Systems Society meeting in Las Vegas on March 6.

"The HTOC is a collaboration between HHS, the Department of Veterans Affairs (VA), and the Defense Health Agency (DHA) to share threat information among federal healthcare providing agencies," Wlaschin said in his slide presentation to the health IT audience.

"CSIRC is the HHS centrally managed incident reporting function that works," Wlaschin said, averaging more than 160 incidents per week,

"CSIRC typically scans against all indicators of compromise (IOCs) -- the unique fingerprints of an incident -- immediately upon receipt and always within 24 hours," according to Wlaschin, while the HCCIC "builds trust by supporting both public and private health sector information security through the establishment and operation" of the center.

Wlaschin credited the HCCIC as "an integral part of the coordinated response to the WannaCry incident. It provided analysis on the WannaCry threat and its impact on health care. HCCIC will strengthen engagement across HHS, increase awareness of healthcare cyber threats, and enhance public-private partnerships through regular engagement and outreach."

Wlaschin has since resigned from HHS as executive director of information security effective March 31, according to news reports.

Also at the HIMSS meeting, the group released its third annual cybersecurity survey which found DHS' NCCIC ranked among the bottom third of sources for cyber threat intelligence for the health sector, with "word of mouth" at the top with nearly 70 percent of respondents.

The overall assessment was that the healthcare sector has "room for improvement" as it has come under increased threats of cyber attacks and as the industry becomes more interconnected and reliant on data to provide basic as well as breakthrough treatment and services.

"Most healthcare organizations' cybersecurity programs have room for improvement," [concludes the annual report](#), which was announced at the HIMSS meeting on March 6. "Significant barriers exist for remediating and mitigating security incidents. Some organizations do not yet have formal insider threat management programs. Risk assessments widely vary from organization to organization," states the report among its top conclusions. -- *Rick Weber*(rweber@iwppnews.com)

