GENERAL COMMITTEE MEETING

Thursday, September 19, 2019
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, **Code:** 30-40-73

1. **Welcome and Introductions**

2. **Guest Speaker** Attachment 1

Deven McGraw
Chief Regulatory Officer
Ciitizen

Biography
Deven McGraw is the Chief Regulatory Officer for Ciitizen. Prior to joining Ciitizen, she directed U.S. health privacy and security policy through her roles as Deputy Director for Health Information Privacy at the HHS Office for Civil Rights (the office that oversees HIPAA policy and enforcement) and Chief Privacy Officer (Acting) of the Office of the National Coordinator for Health IT. Deven also advised PCORNet (the Patient Centered Outcomes Research Network), as well as the federal All of Us Research Initiative, on HIPAA and patient-donated data research initiatives.

Topic: "Health Care Provider Compliance with the HIPAA Right of Individual Access: A Scorecard and Survey"

3. **Legislative Update** Attachment 2

4. **Preliminary Draft of the NIST Privacy Framework** Attachment 3

Save the Date

HAPPY HOUR, Tuesday, September 24 starting at 5:00 pm at Del Frisco's City Center. Confidentiality Coalition and friends – feel free to invite other colleagues who are interested. Celebrating the end of the summer and beginning of fall, gearing up for the rest of the Congressional year. Be there or be square!

WEDI Forum 2019; Emerging Trends and Updates on Privacy and Security in Health IT
Wednesday, October 23, 2019
Jack Morton Auditorium, George Washington University Campus

Health Care Provider Compliance with the HIPAA Right of Individual Access: a Scorecard and Survey

Authors: Deven McGraw, Nasha Fitter, and Lisa Belliveau Taylor*

Abstract

Background: Historically, patients have had difficulty obtaining copies of their medical records, notwithstanding the legal right to do so. In 2018, a study of 83 top hospitals found discrepancies between those hospitals' published information and telephone survey responses regarding their processes for release of records to patients, indicating noncompliance with the HIPAA right of individual access.

Objective: Assess state of compliance with the HIPAA right of access across a broader range of health care providers and in the context of real records requests from patients.

Methods: Evaluate the degree of compliance with the HIPAA right of access 1) by scoring the responses of 51 health care providers to actual patient record requests against the HIPAA right of access requirements and 2) through additional telephone surveys of health care institutions regarding release of records to patients.

Results: Based on the scores of responses of 51 health care providers to record requests and the responses of 3003 healthcare institutions to telephone surveys, more than 50% of health care providers are out of compliance with the HIPAA right of access. The most common failures were refusal to send records to patient or patient's designee by e-mail; health care institutions' responses to telephone survey also indicate 24% are potentially noncompliant with HIPAA's fee limitations. With respect to actual patient record requests, for 71% of providers the records were provided in compliance with HIPAA only after supervisors and privacy officials were educated on HIPAA's requirements.

Conclusions: Recent federal proposals prioritize patient access to medical records through certified electronic health record (EHR) technology, but access by patients to their complete clinical records via EHRs is years away. In the meantime, health care providers need to focus more attention on compliance with the HIPAA right of access, including better training of staff on HIPAA requirements. Greater enforcement of the law will help motivate providers to prioritize this issue.

Introduction

In October 2018, researchers affiliated with Yale University published a study in JAMA Open Network evaluating the processes at 83 top hospitals for responding to patient requests for their medical records under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.[1] The researchers called institutions and inquired about their processes for getting records to patients and compared them to published information about those processes. The study found discrepancies between the records release processes described in the request forms and the description of the process given by institution staff by phone, which indicated noncompliance with HIPAA (as well as applicable state patient record laws).

The study resonated with our own experiences at helping the beta users of Ciitizen obtain their medical records. Ciitizen is a new consumer company developing a personal health record platform to enable patients, beginning with cancer patients, to obtain all of their health information under their HIPAA right of access, allowing them to then share that data to seek second opinions, determine eligibility for clinical trials, and donate data for research. As we began to help the initial beta users of our platform to obtain their medical records using their HIPAA right of access, we recognized widespread noncompliance among health care providers with the HIPAA right of access.

We submitted HIPAA medical requests for records to 51 health care providers, on behalf of 30 cancer patient beta users of the Ciitizen platform, an average of 2.3 medical requests per patient. These were legitimate access requests, on behalf of users who had consented to opening Ciitizen accounts and to having us help them access their health information for the purpose of populating those accounts. We then scored those experiences in comparison to both what is required by the HIPAA right of access, and whether any providers went above and beyond to get patients their records more promptly via a seamless process. As expressed in more detail below, over 50 percent of these providers were either not compliant with the HIPAA right of access or needed multiple phone calls to supervisors or privacy officials to get compliant. Among those providers who were compliant with HIPAA's requirements, we found 18 percent to be going above and beyond what the law requires.

In preparation for submitting those requests, and using a process similar to that used by the Yale researchers, we surveyed, by telephone, thousands of hospitals regarding their processes for releasing medical records pursuant to a patient request. The survey results for 3003 of those hospitals indicated that as many as 56 percent of providers could be out of compliance with HIPAA.

Methodology

The Scorecard: Process

The 30 beta users of the Ciitizen platform came to us through word of mouth (they were individuals either known to or related to Ciitizen staff, were referred by individuals or patient advocacy organizations known to Ciitizen staff, or they signed up on a waitlist). Between February 10, 2019 through July 2, 2019, we submitted written medical records requests, using a HIPAA-compliant form developed by Ciitizen, to providers identified by each user, covering a specific timeframe, requesting all medical records, including images, generated within that timeframe. The records requests were signed by the user (and accompanied by a photo of the user's driver's license, for purposes of proving identity) and submitted by email or by fax, depending on the process acceptable to the provider. The request indicated that the purpose of the request was for continuity of care for a cancer patient. Although patients are not required by HIPAA to identify the purpose for their requests [2], we assumed that including this purpose might help facilitate more rapid fulfillment of those requests. The request also indicated whether the patient further consented to having certain types of sensitive data (for example, genetic information, reproductive health information, HIV/AIDS, and substance abuse treatment information) to be sent, because many providers believe that state or other federal laws require this additional acknowledgement, even for sharing with patients. [3] The request specified that the information be sent directly to Ciitizen by email and expressly acknowledged and accepted the security risks of receiving information unsecurely. (This is required by HIPAA for individuals seeking that their data be sent by unsecure email. [4]) The request also asked for an estimate of any fees associated with completing the request.[5]

Ciitizen staff followed up by phone on each request after it was submitted, to assure that it had been received and that it would be processed in accordance with the request. Staff took careful notes of what occurred during the process, from submission of the request to fulfillment.

The Scorecard: Scoring

The providers to whom the record requests were sent were scored based on one to five stars. The first four stars measure their compliance with core requirements of the HIPAA Privacy Rule right of access, as articulated in the HIPAA privacy regulations and guidance issued by OCR.[6] [7] (Of note, although there are a number of state laws that set a higher bar for patient access to records, we evaluated only compliance with the HIPAA Privacy Rule.) Specifically:

- Provider accepts requests by email or fax: Providers may not create a barrier to access by requiring patients to submit requests in person or by mail.[8]

- Records were sent in the format requested to the patient's designated recipient: The provider sends the records in the format the patient requests, which is in digital form by email (or upload to portal) for text, CD for images), and sends it to the third party designated by the patient.[9]

- Records were sent within 30 days: The provider responds to the request within 30 days of receipt (or, if within 30 days they provided a written statement of reasons for the delay and the date by which the records would be provided, the records were received within 60 days of receipt of the request).[10]

- No unreasonable fees charged for the request: Providers may only charge reasonable, cost-based (i.e., minimal) fees to cover labor costs of copying and supplies.[11]

Providers received one to two additional stars for having seamless processes and for going above and beyond what HIPAA requires to get patients their records. More details on the scoring methodology can be found in Box 1.

Most providers were scored only on a single request; for providers receiving more than one request, we scored/evaluated only the most recent request, as an indication of either improvement or, ideally, consistency in responding to patient requests.

Box 1: Scorecard Scoring

One Star:	Providers earn one star for accepting an access request from a patient by fax or email, which means the provider at least has a HIPAA-compliant process in place for accepting patient record requests (for example, the patient is not asked to mail in a request or make the request in person).
Two Stars:	Providers earn two stars if they ultimately processed the request(s) in a way that met all four of the HIPAA compliant components but did so only after the request had to be escalated (through phone calls) more than once to a supervisor or the provider's privacy official to assure it was fulfilled in compliance with HIPAA. The need for repeated phone calls puts undue burden on the patients requesting their records.
Three Stars:	Providers earn three stars if they meet all four of the HIPAA compliant components with the need for only one escalation phone call to a supervisor or chief privacy officer to educate them on the HIPAA requirements.
Four Stars:	Providers earn four stars if they meet all four of the HIPAA compliant components and process requests without the need for any escalation calls to supervisors or privacy officials.
Five Stars:	Providers who earn five stars go above and beyond to put patients first by sending records in five days or less; accepting an external request form (i.e., not requiring that patients use the provider's specific form); and providing patients their records for free.

The analysis section reports overarching trends for the initial cohort of 51 providers whose responses to HIPAA patient access requests were rated for the scorecard. The scores for each provider can be found at www.patientrecordscorecard.com.

The Survey: Process

In preparation for sending out requests for access on behalf of our users, we searched for a directory of all hospitals and health systems in the U.S. with information about their patient record access processes. We started with hospitals and health systems because they are repositories for a large amount of medical information needed by a cancer patient. No such database currently exists, so we set out to create it. We first attempted to use the Medicare National Provider Identifier (NPI) Database, but found it riddled with duplicates and missing information needed for our purposes. We garnered names of hospitals and health systems by doing Internet searches using phrases such as "top hospitals," "largest health systems in the US," "largest hospital systems in America" "top/largest for-profit hospitals," "top / largest non-profit health systems","top medical centers" and "top cancer centers." Between August 2018 and May 2019, we made phone calls to thousands of hospitals and health systems and had reportable data on 3003. (A large number were difficult to reach by phone (no answer and no return calls to voicemails left on machines), and for others the respondents did not know the answers to the questions, or the responses were too confusing to report or were not reliably recorded.)

Because we were just gathering information to build a database and were not initially setting out to do a systematic investigation of institution responses, the selection is not representative, nor does it constitute a random sample. However, for each institution we used the same script to gather information, with the questions asked matching the HIPAA right of access requirements (see Box 2 for our process and a sample script together with the questions posed to each institution). We realized after building the database that the information constituted an informal survey of hospital and health system patient access request processes and decided there was value to the public in publishing it.

Box 2: Survey Process

1. Call the main switchboard, or, via website information find a direct phone line to the medical records or health information management department. Record number that reaches a live person.
2. Ask "If a patient is out of state and needs copies of their medical records, will you accept a fax or emailed authorization form that includes a copy of their ID and signature?" Record the information as a Y or N; we also recorded the fax and/or email address as appropriate. (We asked the question as an out-of-state patient to assure that we received a response appropriate for remote (not in-person) access.)
3. Ask "If the patient is requesting their medical records be sent electronically (such as by email), are you able to send them their records in that way?" Record the response as Y or N; record N if they refuse to send records to the patient by any means.

4. Ask "Do you charge the patient for their medical records?" If they do charge, ask how much or how they arrive at the charge and record the details.
5. Ask whether radiology imaging can also be requested through the Medical Records Department or if the request needs to be separately made to the Radiology Department/Film Library. For those institutions that indicated they release images only through their Radiology Departments/Film Libraries, call the Radiology Department/Film Library and ask:
    a. If a patient is out of state and needs copies of their actual images, will they accept a fax or emailed request form that includes a copy of their ID and signature?
    b. If they would mail images to patients on a CD (images are too large to send by email).
    c. If they charge patients for images, and if so, how much or by what methodology do they determine the charges.

Institutions were evaluated whether they indicated on the phone that they would accept a request for access (for both records and images) by fax or by email; whether they would send records by email, or images by CD; and whether their purported fees for access were within the bounds of what HIPAA permits. All of these questions address four key aspects of patients right of access under the HIPAA Privacy Rule:

1. the right of a patient to receive records directly (versus sending records only to another health care provider) [6];
2. the right of a patient to submit a request in ways that do not cause undue delay or impose a burden [12];
3. the right of a patient to receive records in the form and format requested, including receiving electronic text records by email [4]; and
4. the right to have any fees for these records be reasonable (reasonable, cost-based fees for the labor needed to make the copy) [13].

Based on their responses, we evaluated whether their responses indicated compliance with HIPAA. Hospitals were deemed to be likely in compliance with HIPAA if their responses to all of the questions were consistent with HIPAA compliance; a noncompliant answer to any question earned the hospital a "no" (N) in the category of indicated compliance with HIPAA.

With respect to fees, the HIPAA Privacy Rule permits health care providers to charge only reasonable, cost-based fees to cover labor costs of copying and any associated supplies.[13] In guidance, OCR sets forth three options for calculating the appropriate reasonable, cost-based fee for the labor associated with making the copy: 1) calculating the actual fee for each request, 2) establishing a fee schedule, such as based on the size of the file, or 3) an easy to apply flat fee of up to $6.50 for digital copies of electronic health records. [14]] OCR guidance also makes clear that per page fees, which are often set forth in state law, are not permitted to be charged for digital copies of digital records.[15]

We evaluated the institutions' responses on fees in the following way:

- We considered an institution to likely be charging "reasonable fees" for patient access if in their responses they stated that they:
    - did not charge patients,
    - charged a flat fee of $6.50 or less for a digital copy (including a copy on CD, even though we were not asking for records in that format), or
    - reported fees that seemed to be based on reasonable labor costs for copying (for example, by responding that the costs were $X per hour of copying).
- We considered an institution to likely be charging "unreasonable fees" if in their responses they stated that they:
    - charged per page fees (even if initial pages were free), including any fees for records retrieval, or
    - charged a flat fee higher than $6.50.
- Institutions who did not answer this question, or whose responses were too confusing to evaluate, are reported as NA (not applicable). We removed all institutions with NA from the denominator in calculating the percentage of institutions whose responses indicated compliance with this aspect of the HIPAA right of access.

Because this is based on phone inquiries, and not a response to an actual request, we were unable to evaluate whether records would be provided within HIPAA's 30-day timeline or whether the records would be sent to a third party designee.[16] [17] We are also deeming these responses to be "indications" of compliance or noncompliance because they are not responses to an actual records request submitted by a patient.

The analysis section reports some overarching trends among the institutions who responded to our queries. Detailed survey results for each institution surveyed can be found at www.patientrecordsscorecard.com.

Analysis

The Scorecard

51 healthcare providers were scored based on how they processed an individual access request in compliance with HIPAA (Figure A):

Figure A: Compliance with HIPAA (n=51 Healthcare Providers)

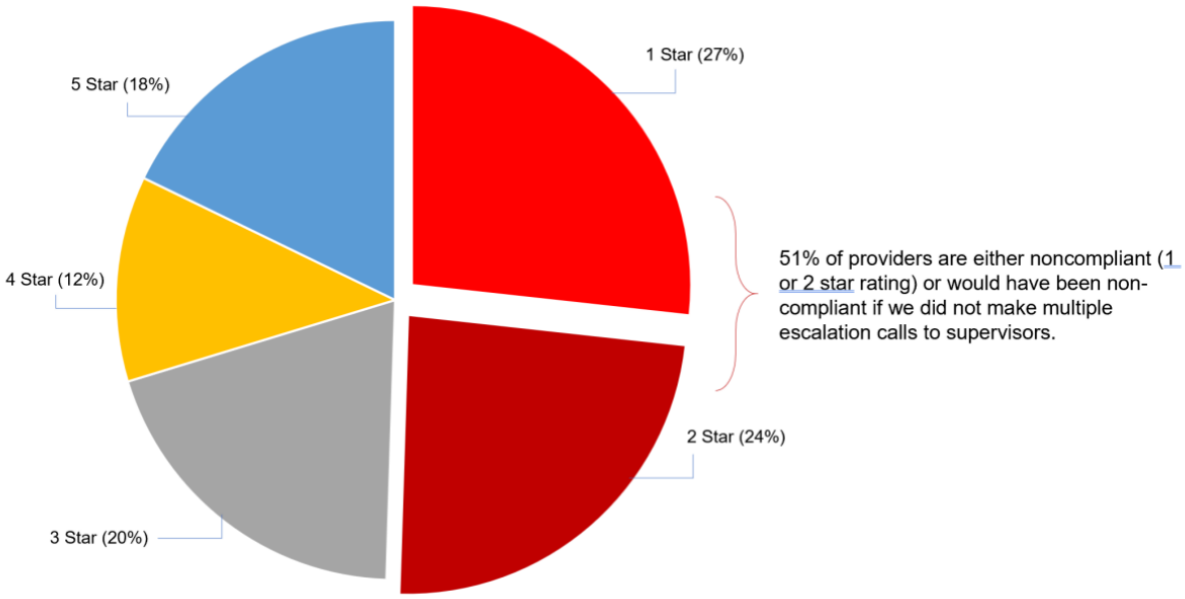


Figure A: Compliance with HIPAA based on 51 surveyed healthcare providers

Main Reason for Noncompliance: Providers Don't Send Records in the Form and Format Requested by the Patient (Email for text records)

The primary reason for noncompliance is that healthcare providers do not send records electronically when explicitly requested in that format by the patient. Of the 14 healthcare providers receiving one star, 12 of them (86%) failed for not providing records in the electronic form and format requested by the patient (by unsecure email for text records). (One healthcare provider was noncompliant for failing to send records to the patient's designee; the other was noncompliant for charging unreasonable fees.) Providers and their copy services continue to send paper records, faxes and CDs - even when the patient explicitly requests records be sent electronically to a designee over email or uploaded to a portal. Healthcare providers are also hesitant to send records by standard (unsecure) email, even pursuant to specific patient requests that include acknowledgement and acceptance of security risks. Figure B below shows the various ways patient records were sent.

Figure B: Methods of Delivery of Medical Records
(n=14 Healthcare Providers Receiving One Star)

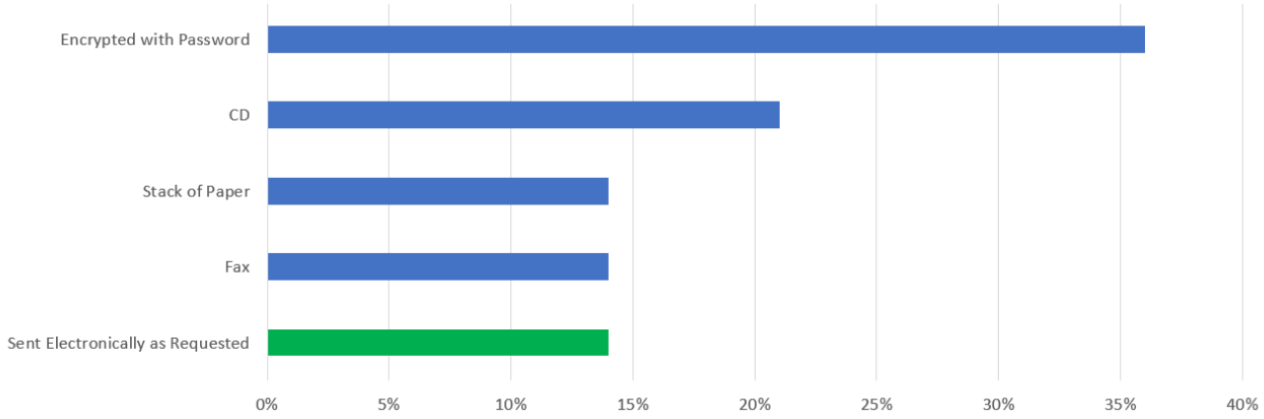


Figure B: Methods of delivery of patient records requests

Additional Significant Compliance Risk - Staff Lack of Knowledge of HIPAA Requirements

It took our team between one and 26 days to fulfill patient requests, with eight days as the average (Table 1). Without at least some learned intervention - ranging from educating staff on HIPAA requirements up to escalation calls to supervisors and privacy officials - **71% of these requests would not have been fulfilled pursuant to HIPAA requirements.** We followed an outreach process to medical records offices:

- Confirming request for records was received;
- Following up, answering questions, explaining HIPAA requirements; and
- Escalating to supervisors and/or privacy officers.

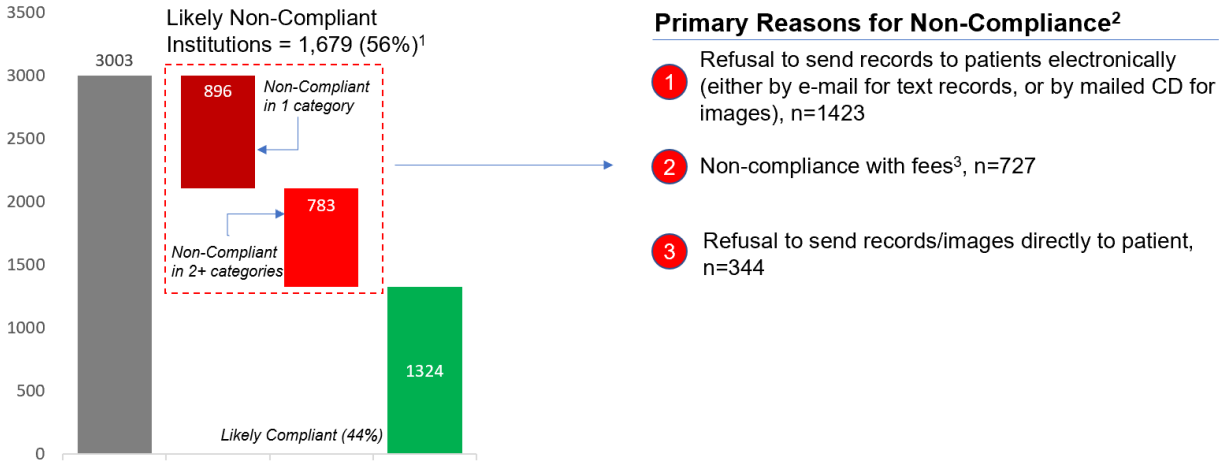
	Confirmation Calls per Request	Medical Records Office Follow-Up Calls per Request	Escalation Calls per Request	Total Calls per Request
Average	2	3	2	7
Maximum	6	8	10	24

Table 1: Average and maximum events for outreach to medical records offices

The Survey

We conducted a phone survey of thousands of health care institutions to assess likelihood of compliance if patient requests were made to their offices (see Fig C); we obtained reportable data on 3003 institutions. Overall, 56% (n=1,679) of institution responses indicated noncompliance with the HIPAA right of access, with 783 of those institution responses (47%) indicating noncompliance in two or more categories. Similar to results we saw on our scorecard analysis when submitting actual patient requests, refusal to send records to patients electronically by email was a primary reason for likely noncompliance. In the survey, noncompliant fee responses was the second highest reason for potential noncompliance.

Figure C: Phone Survey Findings



Notes:
(1) Noncompliance in at least one category indicates overall noncompliance. This is because all components are legally required to be compliant
(2) Institutions can be non-compliant for more than one reason
(3) We also found that of the 727 institutions non-compliant with fees, 521 (72%) were also non-compliant in another category

A number of institutions route patient access requests for images directly to their Radiology Departments or Radiology Film Libraries (collectively, "Radiology"). In comparing the responses of medical records departments to those of Radiology, medical records department responses were over four times more noncompliant than those of Radiology. However, of the 344 institutions whose responses indicated noncompliance regarding willingness to send information directly to the patient (responding they would send information only to another provider), 77% of the noncompliant responses came from Radiology.

Most institutions (n=2,616, 87%) responded that they would accept a request from patients sent by email or fax.

In 2016, OCR released extensive guidance on the HIPAA right of access that included a significant emphasis on fees. [15] We speculated that if an institution's answer to the fee question indicated noncompliance, it was likely the institution was noncompliant in another category, using the fee issue as a proxy for whether the institution was generally up-to-date on their HIPAA right of access obligations. Our survey showed 72% (521/727) of providers whose responses indicated noncompliance with the fee provisions also had responses indicating noncompliance with another aspect of the right of access.

Discussion

The scorecard and survey data collectively demonstrate that we have a long way to go to achieve consistent, seamless and HIPAA compliant processes for getting records to patients. As seen below, the results from the broad survey of 3003 institutions, and the actual responses to patient requests by 51 providers, yielded similar results:

	Scorecard	Survey
Overall Noncompliance/Compliance Only with Multiple Interventions	51%	56%
% of Noncompliant (or Likely Noncompliant) Providers Refusing to Send Records Electronically by Email	85%	85%

One distinction between the survey and scorecard results worth noting: the institutions' responses on the survey indicated that 24 percent were likely noncompliant with the fee provisions of the HIPAA Right of Access. However, only one of the 51 providers evaluated in the scorecard was noncompliant due to noncompliant fees. We believe the amount of time spent on the phone with medical records staff, supervisors and privacy officials at scorecard providers to assure the requests were processed in compliance with HIPAA was a significant factor in assuring that only lawful fees were charged.

The privacy regulations under HIPAA have always included a right of individuals to access and receive copies of their complete medical records, with rare exceptions. In the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), Congress clarified that individuals have the right to digital copies of electronic health records and to have those copies sent directly to a designated third party, such as a personal health record service or mobile health application (app). [18]] The Department of Health and Human Services (HHS) incorporated the HITECH changes into the HIPAA Privacy Rule in 2013. [19] These changes to the HIPAA Privacy Rule right of access were part of an emphasis in HITECH on digital collection and exchange of health information and were expected to spark the development of more widespread personal health record services and mobile applications designed for use by individuals.

Notwithstanding the long history of this right, individuals have long struggled to exercise it. Inability to exercise the right of access has always been one of the top five categories of complaints to the HHS Office for Civil Rights (OCR), the office with authority to promulgate policy under and enforce HIPAA's privacy mandates. [20] In 2016, complaints about inability to access records were, for the first time, the top category of complaints, surpassing inappropriate uses and disclosures for the first time.[20]

Customarily, individuals seeking copies of their medical records have had to submit requests on paper (or digitized paper) forms to medical records departments. The records, when produced, would be mailed (or sometimes faxed) to patients, or placed on a CD. Individuals often were required to pay fees – sometimes significant fees – to obtain their records. [21] However, recent federal efforts are pushing in the direction of enabling individuals to seamlessly access their health information online. Beginning with portals in certified electronic health record systems, coupled with incentive payments for providers to make data available to patients in those portals, and extending to more recent proposals for individuals to have an increasing amount of their health information available to them, via the app of their choice, through open standard application programming interfaces (APIs) and potential penalties for "blocking" information access by patients, the future of patient empowerment through seamless access to their health information is in sight.

These efforts – while promising – will take years to fully implement. The proposed timeline to implement APIs is two years after a final rule is published, and health care providers and EHR vendors are asking for more time.[22] Today, portals in EHRs are required to expose the data comprising the Common Clinical Dataset. [23] This is a good set of data – but it is significantly shy of all of the information that an individual has a right to under HIPAA. For example, it does not include images, notes, pathology reports, genomic/genetic test data. Federal officials have announced a glide path for expanding the data required to be accessible to patients via APIs - but this process will take years.[24] Consequently, patients seeking copies of all of their health records likely will need to obtain those records through a combination of digital access through APIs and the traditional route of submitting requests to medical records departments, which makes compliance with the HIPAA right of access by medical records departments and Radiology of continuing importance.

It appears from this study that training of medical record department and Radiology staff is critical to assuring that patient requests are processed in accordance with the HIPAA Privacy Rule. The number of phone calls required to get a request processed in accordance with HIPAA strongly suggests that the average patient - not necessarily armed with textbook knowledge of the HIPAA requirements - would likely be far less successful at getting their requests processed in compliance with the law and might give up due to lack of time or frustration. (OCR Director Roger Severino publicly shared that he gave up on his efforts to obtain his own medical records. [25]) In particular, the requirement to send information to patients (or their designees) in the form or format the patient requests – including by email (or CD for images) – is an aspect of the HIPAA right of access that needs to be reinforced. Although overall the actual performance by

scorecard providers on the fee limitations was much better than expected given the survey data, this is still an area that providers also need to evaluate to assure they are in compliance with the law.

In conclusion, with more than 50% of providers either out of compliance or at significant risk of noncompliance, the rights of patients to their health records is still being violated by too many health systems. Although many entities, including ONC and OCR, are working to educate patients and providers, additional enforcement of the right of access by OCR is needed.

We engaged in this study not to name and shame but to educate hospitals and other providers on the extent of noncompliance with the HIPAA Right of Access that exists – and the need for all HIPAA covered entities to examine their processes and assure compliance with the HIPAA Right of Access.

We also wish to highlight for policymakers just how difficult it continues to be for patients to access their health information. Efforts to digitize this process have been proposed, but it will be years before seamless digital access by patients to all of their health information is a reality. In the meantime, requests to medical records departments (and Radiology) will still be required to enable patients to amass all of their health information. It is critical that these processes be compliant with HIPAA and responsive to patient needs.

Ethical Review

The scorecard and survey do not constitute human subjects research under HIPAA or the Common Rule. The scorecard is retrospectively evaluating the responses of health care institutions to Ciitizen users' requests for medical records that were processed by Ciitizen staff. Ciitizen users expressly consented to Ciitizen assisting in the gathering of their medical records; also, as part of the consent that each user executes to open a Ciitizen account, users were required to assent to Ciitizen's privacy policy, which makes clear that Ciitizen can publish aggregate statistics about use of Ciitizen services.[26] The survey retrospectively evaluated institutional policies on patient record access based on telephone responses; the survey was evaluating the institutions, not the individuals responding to the call.

Limitations

This study has several limitations. The survey data was gathered by Ciitizen staff, including temporary staff added just for purposes of compiling the survey data. We instructed all surveyors to use the script (see Box 2) but we did not record the calls, nor were the surveyors supervised or monitored in making these calls. Also, because the responses on fees were so varied, we did not have conventions/standards for surveyors to follow in recording their information. We also acknowledge that responses could be mis-recorded by staff. These are all reasons why we are reporting the survey data as *indicating* compliance or noncompliance. Given that the information we received in the survey could have been provided to any patient

randomly calling with the same questions, we still believe the survey results could be instructive to hospitals in terms of assuring that proper information about HIPAA right of access processes is being provided to the public.

The scorecard was created for this study and is not an established instrument; it was based on actual patient requests to hospitals. Here our involvement to get these requests processed was extensive, as the requests needed to be escalated, sometimes with multiple phone calls. This suggests that the experience of a patient, without any help, could have been worse. Institutions did not realize at the time that they were being evaluated on their processes, so it is appropriate to consider this as an experience that could have happened to any patient.

In both the scorecard and survey, we listed providers separately by location. Although health care providers have the option under the HIPAA Privacy Rule to consolidate HIPAA compliance responsibilities for all of their locations under a central office [27], they are not required to do so – and unraveling those corporate relationships, which often change, would have been difficult, if not impossible, to do. Since the experience of a patient in requesting their health information is to query the location where they received care, we believe the scorecard and survey more accurately represents what a patient would experience if they made an access request or inquired about making one.

References

* Deven McGraw is the Chief Regulatory Officer of Ciitizen Corporation (formerly Deputy Director for Health Information Privacy at the Office for Civil Rights at the federal Department of Health and Human Services); Nasha Fitter is the Director of Patient Experience at Ciitizen Corporation; Lisa Belliveau Taylor leads patient access request processing at Ciitzen Corporation.

1. Lye CT, Forman HP, Gao R, Daniel JG, Hsiao AL, Mann MK, deBronkart D, Campos HO, Krumholz HM. Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records. JAMA Netw Open 2018 Oct5; 1(6):e183014. PMID: 30646219.
2. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html (see section on "Grounds for Denial").
3. See, for example, https://stanfordhealthcare.org/for-patients-visitors/your-hospital-stay/medical-records.html and https://www.texasmedclinic.com/wp-content/uploads/2017/07/medical-records-request121615pdf.pdf.
4. https://www.hhs.gov/hipaa/for-professionals/faq/2060/do-individuals-have-the-right-under-hipaa-to-have/index.html
5. https://www.hhs.gov/hipaa/for-professionals/faq/2028/must-a-covered-entity-inform-individuals-in-advance/index.html
6. Title 45 Code of Federal Regulations (CFR) Section 164.524.
7. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
8. 45 CFR 164.524(b)(1) and https://www.hhs.gov/hipaa/for-professionals/faq/2036/can-an-individual-through-the-hipaa-right/index.html)
9. 45 CFR 164.524(c)(2)(ii) & (c)(3)(ii) and https://www.hhs.gov/hipaa/for-professionals/faq/2036/can-an-individual-through-the-hipaa-right/index.html)
10. 45 CFR 164.524(b)(2)(i).
11. 45 CFR 164.524(c)(4).
12. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html (see section on "Unreasonable Measures").
13. https://www.hhs.gov/hipaa/for-professionals/faq/2024/may-a-covered-entity-charge-individuals-a-fee/index.html
14. https://www.hhs.gov/hipaa/for-professionals/faq/2029/how-can-covered-entities-calculate-the-limited-fee/index.html
15. https://www.hhs.gov/hipaa/for-professionals/faq/2031/are-costs-authorized-by-state-fee-schedules-permitted/index.html
16. 45 CFR 164.524(b)(2)(i).
17. 45 CFR 164.524(c)(3)(ii).
18. Health Information Technology for Economic and Clinical Health Act, enacted as title XIII of division A and title IV of division B of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5), Section 13405(e)(1).
19. Vol. 78 No. 17 Federal Register, pages 5566-5702 (Jan. 25, 2013).
20. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/top-five-issues-investigated-cases-closed-corrective-action-calendar-year/index.html

21. Jaspers AW, Cox JL, Krumholz HM. Copy Fees and Limitations of Patients' Access to Their Own Medical Records. JAMA Intern Med. 2017;177(4):457-458. PMID: 28135350.
22. See, for example, https://www.fiercehealthcare.com/tech/complying-information-blocking-rule-will-be-a-challenge-without-standardized-apis-himss, https://www.healthdatamanagement.com/news/onc-cms-proposed-rules-continue-to-come-under-fire-from-stakeholders, & https://www.ama-assn.org/system/files/2019-06/executive-summary-onc-proposed-rule.pdf.
23. https://www.healthit.gov/sites/default/files/commonclinicaldataset_ml_11-4-15.pdf
24. https://www.healthit.gov/sites/default/files/draft-uscdi.pdf
25. https://www.politico.com/newsletters/morning-ehealth/2019/02/14/himss-news-ocr-enforcement-coming-393826; https://twitter.com/HealthPrivacy/status/1095380112835518464?s=20
26. http://www.ciitizen.com/privacy/
27. 45 CFR 164.105(b).

Federal data privacy proposals

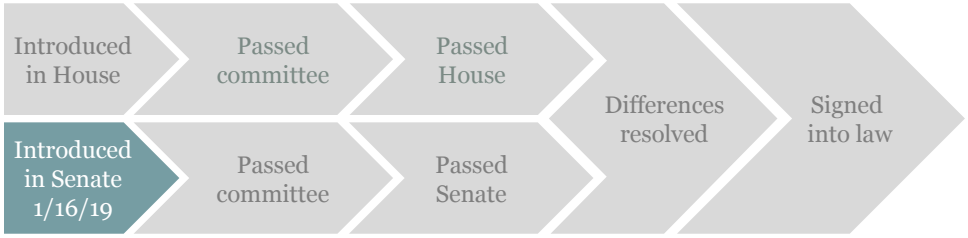
An overview of privacy proposals introduced in the 115th and 116th Congresses

Legislation tracker: data privacy in the 116th Congress

S. 142: American Data Dissemination Act

Sponsor: Sen. Marco Rubio (R-FL)

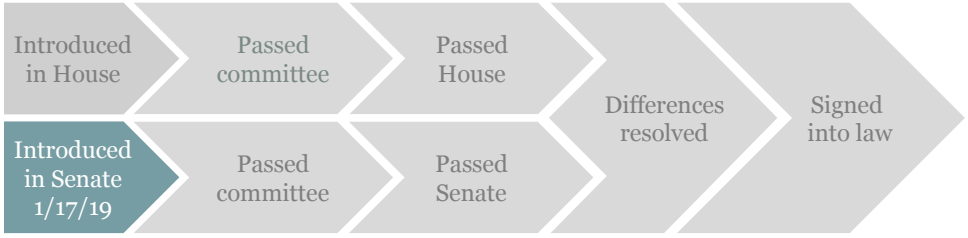
- Requires the FTC to provide Congress with recommendations for privacy legislation for Internet Service Providers within six months, using the 1974 Privacy Act as a framework
- Authorizes the FTC to create privacy regulations based on the Privacy Act, should Congress fail to act on the FTC's recommendations within two years; with exceptions for newer or smaller companies



S. 189: The Social Media Privacy Protection and Consumer Rights Act

Sponsors: Sen Amy Klobuchar (D-MN)

- Requires companies to report data breaches to consumers within 72 hours of discovery
- Requires companies to inform consumers that their personal data will be collected by operators or third parties, and allows access to the data collected
- Allows users to opt out of data collection, but permits companies to deny products or services if the users' privacy options are not operable



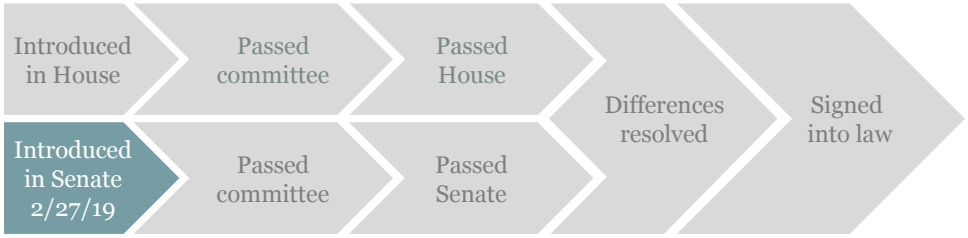
Sources: Congress.gov; Sen. Marco Rubio, "Congress needs to address consumer data privacy in a responsible and modern manner," The Hill, Jan. 16, 2019; "The American Data Dissemination Act," Marco Rubio Press Release, January 16, 2019.

Legislation tracker: data privacy in the 116th Congress

S. 583: DATA Privacy Act

Sponsor: Sen. Catherine Cortez Masto (D-NV)

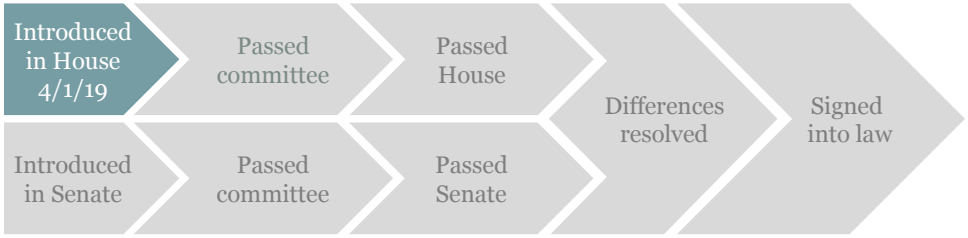
- Would require businesses to offer opt-out consent in all reasonable cases, as well as opt-in consent for sensitive data or data for non-business purposes
- Would require businesses that collect data from 3,000+ people and generate over $25 million annually to appoint a privacy protection officer
- Would support National Science Foundation research into privacy-enhancing technology



H.R. 2013: Information Transparency and Personal Data Control Act

Sponsor: Rep. Suzan DelBene (D-WA-1)

- Would require businesses to obtain opt-in consent before collecting and using sensitive personal data
- Would authorize the FTC to issue monetary penalties for first offenses
- Would require businesses to undergo biannual third-party privacy audits and report the results to the FTC



Sources: Congress.gov

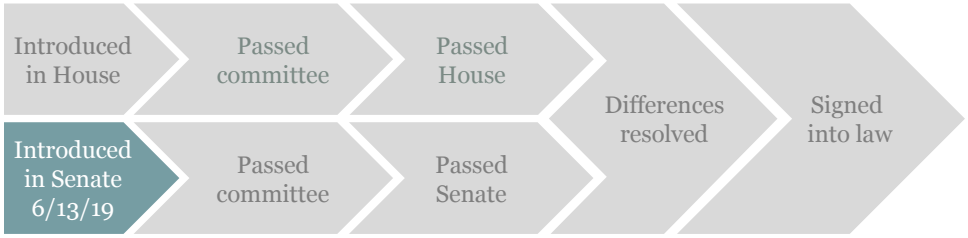
Slide last updated on: July 22, 2019

Legislation tracker: data privacy in the 116th Congress

S. 1842: Protecting Personal Health Data Act

Sponsor: Sen. Amy Klobuchar (D-MN)

- Would create regulations within the FTC on the collection, processing, analysis, or other use of personal health data
- Would establish a National Task Force on Health Data Protection to oversee and provide input on regulations related to genetic or biometric health data
- Would require a report to congressional stakeholders on the findings of the Task Force one year after its creation on proper practices related to personal health data protection



Sources: Congress.gov

Slide last updated on: July 22, 2019

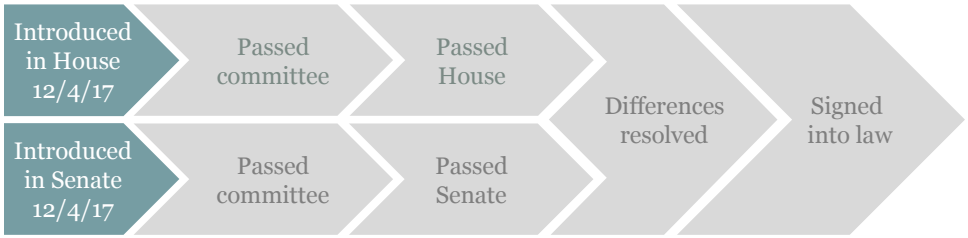
Legislation tracker: data privacy in the 115th Congress

H.R. 4543/S. 2187: Commercial Privacy Bill of Rights Act of 2017 (short title)

House Sponsor: Rep. Albio Sires (D-NJ-08)

Senate Sponsor: Sen. Robert Menendez (D-NJ)

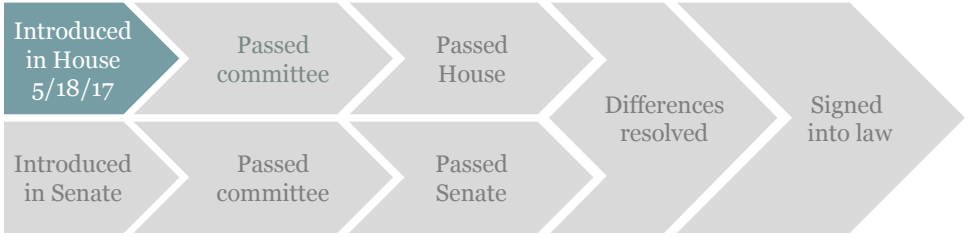
- Amends the Children's Online Privacy Protection Act of 1998 to improve provisions relating to collection, use, and disclosure of personal information of children



H.R. 2520: BROWSER Act of 2017

Sponsor: Rep. Marsha Blackburn (R-TN-07)

- Reinstates the FCC's Obama-era internet privacy rules that prohibit ISPs from sharing or selling individuals' personal data without their consent — Congress voted in 2017 to repeal the FCC's rules
- Extends the FCC's rules to apply to companies such as Google and Facebook , which were not subject to the rules before
- Establishes the FTC as the enforcer of internet privacy rules



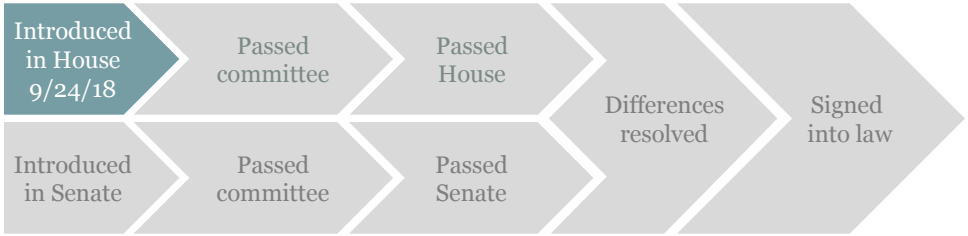
Sources: Congress.gov, 2019; Govtrack.us, 2019.

Legislation tracker: data privacy in the 115th Congress

H.R. 6864: Information Transparency & Personal Data Control Act

Sponsor: Rep. Suzan DelBene (D-WA-01)

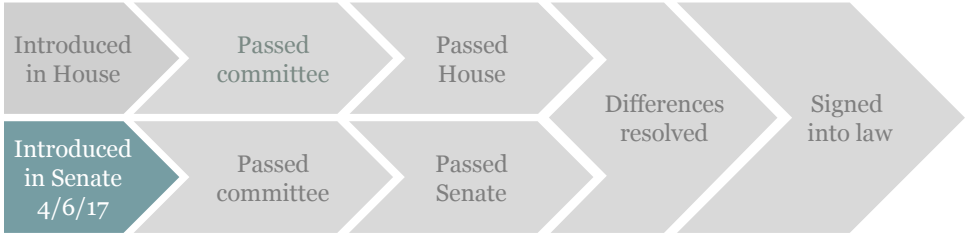
- Requires companies to obtain opt-in consent before collecting and using sensitive personal data
- Requires companies to notify consumers if and with whom their personal data is being shared as well as the purpose of disseminating such data
- Provides rulemaking authority to the FTC



S. 878: A bill to establish privacy protections for customers of broadband Internet access service and other telecommunications services

Sponsor: Sen. Edward Markey (D-MA)

- Amends the Communications Act of 1934 to require ISPs to notify individuals about the collection, use, and sharing of personal data
- Require ISPs to obtain opt-in consent before using and sharing sensitive personal data



Sources: Congress.gov, 2019; Govtrack.us; "DelBene Introduces Legislation to Regulate Consumer Privacy," Suzane DelBene Press Release, September 20, 2018; "Senator Markey Leads Senators in Legislation to Fully Restore Broadband Privacy Protections," Edward Markey Press Release, April 7, 2017.

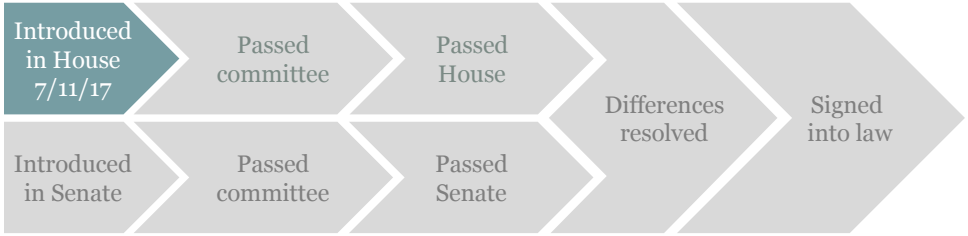
Slide last updated on: March 20, 2019

Legislation tracker: data privacy in the 115th Congress

H.R. 3175: Online Privacy Act

Sponsor: Rep. Keith Ellison (D-MN-5)

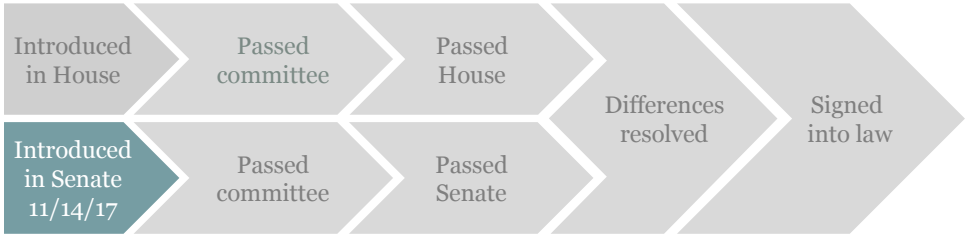
- Amends the Communications Act of 1934 to require ISPs to notify individuals about the collection, use, and sharing of personal data
- Requires ISPs to obtain opt-in consent before using and sharing sensitive personal data



S. 2124: Consumer Privacy Protection Act of 2017

Sponsor: Sen. Patrick Leahy (D-VT)

- Requires companies to meet certain baseline standards for consumer privacy and data security
- Requires companies to notify consumers when a data breach occurs



Sources: Congress.gov, 2019; Govtrack, 2019; "Leahy Introduces The Consumer Privacy Protection Act," Patrick Leahy Press Release, November 11, 2017.

Slide last updated on: March 20, 2019

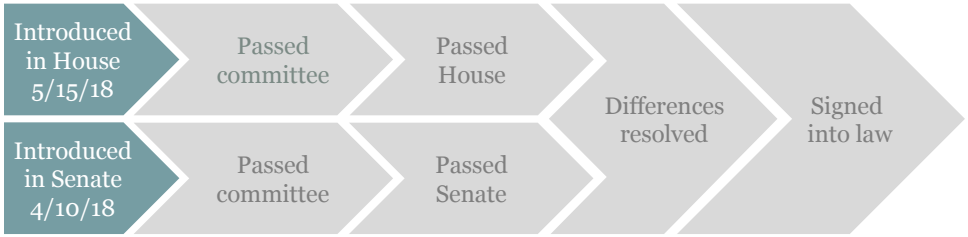
Legislation tracker: data privacy in the 115th Congress

S. 2639/H.R. 5815: CONSENT Act

House Sponsor: Rep. Michael Capuano (D-MA-07)

Senate Sponsor: Sen. Edward Markey (D-MA)

- Requires edge providers, such as Facebook and Google to obtain opt-in consent from consumers to use, share, or sell personal data
- Requires edge providers to implement reasonable data security practices
- Requires edge providers to notify consumers about any collection, use, and sharing of personal data
- Requires edge providers to notify consumers when a data breach occurs
- Authorizes the FTC to enforce these regulations

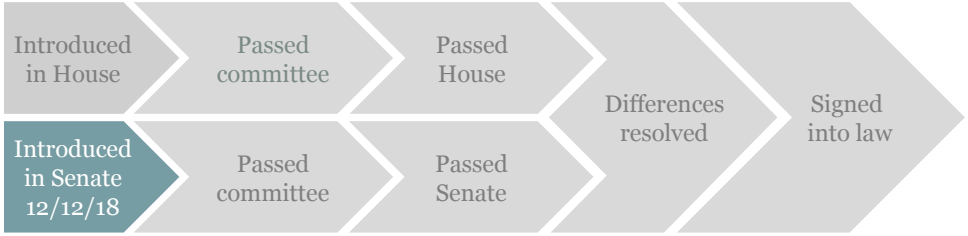


S. 3744: Data Care Act of 2018

Sponsor: Sen. Brian Schatz (D-HI)

Establishes "duties" that require ISPs to protect consumer data and privacy:

- Duty of Care — ISPs reasonably secure personal data and notify consumers if a data breach occurs
- Duty of Loyalty — ISPs must not use data in a way that harms consumers
- Duty of Confidentiality — ISPs must ensure that the duties of care and loyalty apply to third parties when sharing or selling personal data
- Authorizes the FTC to enforce these regulations



Sources: Congress.gov, 2019; "As Facebook CEO Zuckerberg Testifies to Congress, Senators Markey and Blumenthal Introduce Privacy Bill of Rights," Edward Markey Press Release, April 10, 2018; "Schatz Leads Group of 15 Senators in Introducing New Bill to Help Protect People's Personal Data Online," Brian Schatz Press Release, December 12, 2018.

Key privacy principles

Since the passage of GDPR and CA privacy law, several organizations and lawmakers have released proposed policy recommendations for a federal privacy law, which generally cover these key concepts:

Enforcement

1. Federal preemption

Should federal or state regulators be responsible for enforcing privacy laws?

2. Regulatory scope

Should a privacy law apply equally to all industries, technologies, and sizes of companies?

3. Regulatory flexibility

Should the law draw a clear distinction between required protections and treatment of "personal data" vs. "sensitive personal data?"

Corporate responsibility

1. Transparency

What responsibilities should companies have to inform consumers regarding data collection, use, and sharing?

2. Collection limits

Should there be restrictions on the types of data that companies are allowed to collect?

3. Data breach notification

Should there be a single federal standard for notifying consumers in the event of a data breach?

Consumer rights

1. Right to access, modify, export, and delete

What types of rights should consumers have to access, modify, export, and delete their data?

2. Consent

Should consumers have to provide explicit consent for companies to collect any personal data? What mechanism of consent is necessary?

3. Private right of action

Should the law enable consumers to sue an organization directly for civil penalties if that entity violates the privacy law?

Sources: "Section-by-Section Analysis and Explanation Consumer Data Protection Act of 2018" Sen. Ron Wyden, November 2018; "An Ethical and Innovative Privacy Law," Intel Corporation, January 28, 2019; "Model Privacy Legislation," US Chamber, February 2019.

Trends in selected privacy proposals

Draft legislation from Sen. Ron Wyden (D-OR), the US Chamber of Commerce, and Intel reach consensus on these broad themes:

Federal baseline standards

There is an urgent need for a federal law that:

- Establishes baseline cybersecurity and privacy standards
- Ensures strong privacy protections while promoting innovation

Transparency

Companies should be required to be transparent with consumers about:

- The type of personal data they have collected
- The purpose for its collection
- If and when their data is being shared

Expanded FTC Authority

The FTC should have expanded authority and resources to:

- Create and implement privacy rules
- Address threats to consumer privacy
- Enforce penalties for violations

Consumer control

Consumers should have more control over their personal data, and should have opportunities to:

- Access and correct inaccuracies in data that a company has collected about them
- Make informed choices about their data (opt-in/opt-out)

Sources: "Section-by-Section Analysis and Explanation Consumer Data Protection Act of 2018" Sen. Ron Wyden, November 2018; "An Ethical and Innovative Privacy Law," Intel Corporation, January 28, 2019; "Model Privacy Legislation," US Chamber, February 2019.

Comparison of proposed federal privacy bills

The proposals have differing policy recommendations for key privacy principles

Principle	Sen. Wyden proposal	US Chamber proposal	Intel proposal
Federal preemption	• **Does not preempt** any existing state data security & privacy laws, **including data breach notification laws**	• **Preempts** any existing state data security & privacy laws, **including data breach notification laws**	• **Preempts** any existing state data security & privacy laws**, except for data breach notification laws**
Enforcement	• **Expands the FTC's powers** and resources, but does not provide authority to preempt state laws	• **Establishes the FTC** as the primary enforcer of the regulations	• **Establishes the FTC** as the primary enforcer of the regulations
Scope	• **Applies only to companies** with over $50M in avg. annual revenue or data on at least 1M consumers • Does not address sector neutrality	• **Sector neutral –** applies equally across all industry sectors	• **Applies to all companies** under the FTC's authority, except for organizations with fewer than 25 employees and those that collect personal data from fewer than 50,000 individuals
Consent	• **Opt-out –** requires companies to honor requests to not share consumers' personal data with third-parties	• **Opt-out –** requires companies to honor requests to not share consumers' personal data with third-parties	• **Tailored –** requires corporations to provide explicit notice **("opt-in")** when collecting sensitive data, but not necessarily for other types of data
Penalties	• **Enforces fines** of up to 4% of annual revenue for a company's first offense and imprisonment of up to 20 years for noncompliance	• **Does not specify fines** or other penalties for noncompliance	• **Enforces fines** of up to $1M and imprisonment of up to 10 years for noncompliance
"Safe harbor"	• **Does not include a safe harbor**	• **Includes a safe harbor** for companies that certify they are in compliance	• **Includes a safe harbor** for companies that certify they are in compliance

Sources: "Section-by-Section Analysis and Explanation Consumer Data Protection Act of 2018" Sen. Ron Wyden, November 2018; "An Ethical and Innovative Privacy Law," Intel Corporation, January 28, 2019; "Model Privacy Legislation," US Chamber, February 2019.

NIST Requests Comments on Draft Privacy Framework

Document provides guidance to help organizations protect individual privacy.

September 09, 2019

Protecting our privacy while keeping the digital wheels of society turning may feel mutually exclusive at times, but a new tool from the National Institute of Standards and Technology (NIST) may help all of us — individuals and organizations alike — breathe a bit easier.

The agency has just released the preliminary draft of the *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management.* The document aims to help organizations with a tricky task: maximizing beneficial uses of data while minimizing privacy problems for individuals. While data can enhance airport security, develop social connections, or serve myriad other positive purposes, inadequate data management can result in a range of problems for individuals. In turn, these problems can affect an organization's reputation and bottom line.

Based on nearly a year of extensive public conversations, the NIST Privacy Framework provides guidance for organizations that need to develop strategies to minimize privacy risks while still accomplishing their missions. It also provides a way for organizations to have productive dialogues about privacy risks arising from their products or services.

"We see privacy as something that safeguards human values, like dignity and autonomy," said Naomi Lefkovitz, a senior privacy policy adviser at NIST and leader of the framework effort. "It's a challenging topic, though, because we have so many individual and societal conceptions of what privacy means."

Privacy as a fundamental American value reaches back to the U.S. Constitution's Fourth Amendment, Lefkovitz said, but when it comes to digital information, protecting it can mean controlling personal information or hiding it from easy view. An organization might use cryptography, for example, or de-identification techniques to limit the inferences that can be made about people from their online behavior or digital transactions.

Because there are many valid methods of achieving privacy, the framework offers organizations the option of choosing different types of protection outcomes, ones that suit their business environments and allow them to meet the privacy needs of individuals who use their services.

Privacy is a concept distinct from security, but the two are intimately connected in our digital world. A security breach that cracks a company's database might reveal private information about thousands of individuals. For that reason, many industry stakeholders

over the past year requested that NIST align the Privacy Framework with the Cybersecurity Framework, one of NIST's flagship publications.

The Privacy Framework is therefore aligned with the Cybersecurity Framework both structurally and conceptually, and they are designed to be used together.

Both documents help organizations assess their own risks and achieve their particular goals. Similar to the Cybersecurity Framework structure, the Privacy Framework centers on three parts:

- The *Core* offers a set of privacy protection activities and enables a dialogue within an organization about the outcomes it desires.
- *Profiles* help determine which of the activities in the Core an organization should pursue to reach its goals most effectively.
- *Implementation Tiers* help optimize the resources dedicated to managing privacy risk. One company might have more risks, for example, and might need to have a chief privacy officer, while another might not.

Lefkovitz emphasized that the framework is not a simple one-size-fits-all checklist of action items.

"A checklist-based approach might make you overinvest in less effective privacy solutions for your situation or underinvest in the ones that would give you the most privacy benefit," Lefkovitz said. "The framework is designed to help your organization recognize and then address its own potentially unique situation."

NIST has posted a notice in today's *Federal Register* and will accept public comments on the draft Privacy Framework until 5 p.m. EDT on Oct. 24, 2019. The NIST authors plan to update the draft framework based on public feedback before issuing a version 1.0, expected by the end of 2019.

"Privacy risk management practices are not yet well understood," Lefkovitz said. "This document is just a beginning. In collaboration with our stakeholders, we will build more guidance around it."

Information Technology, Cybersecurity and Privacy