

HHS OCR

2021 NEHIA Conference

Office for Civil Rights (OCR)
U.S. Department of Health and Human Services



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

Policy

Proposed Modifications to the HIPAA Privacy Rule to Empower Patients, Improve Coordinated Care, and Reduce Regulatory Burdens

- The NPRM solicits public comment on proposals to modify the HIPAA Privacy Rule to improve health information sharing for more effective health care, empower individuals with their own health information, and lift unnecessary burdens on covered health care providers and health plans.
- OCR HIPAA NPRM Fact Sheet
 - <https://www.hhs.gov/sites/default/files/hipaa-nprm-factsheet.pdf>
- The NPRM was published in the Federal Register on January 21, 2021.
- The public comment period closed on May 6, 2021.
- Comments are now available for public viewing at <https://www.regulations.gov/document/HHS-OCR-2021-0006-0001>.

HIPAA and COVID-19 Updates

- February Bulletin on HIPAA and COVID-19
- Notification of Enforcement Discretion on Telehealth Remote Communications
- Guidance on Telehealth Remote Communications
- Guidance on Disclosures to Law Enforcement, Paramedics, Other First Responders, and Public Health Authorities
- Notification of Enforcement Discretion on Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities
- Notification of Enforcement Discretion Regarding COVID-19 Community-Based Testing Sites
- Guidance on Media and Film Crew Access to Protected Health Information
- Guidance on HIPAA and Contacting Former COVID-19 Patients about Plasma Donation
- Guidance on HIPAA, Health Information Exchanges, and Disclosures of PHI for Public Health Purposes
- Notification of Enforcement Discretion for Use of Online or Web-Based Scheduling Applications for the Scheduling of COVID-19 Vaccination Appointments

February Bulletin on HIPAA and COVID-19

- How patient information may be shared without a HIPAA authorization
 - Treatment
 - Public Health Activities
 - Family, Friends, and Others Involved in an Individual's Care or Payment for Care
 - To Prevent or Lessen a Serious and Imminent Threat
- Cautions against disclosures to the media
- Reminds about the minimum necessary standard and reasonable safeguards

<https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf>

Notification of Enforcement Discretion on Telehealth Remote Communications

- OCR will not impose HIPAA penalties against covered health care providers for noncompliance in connection with the good faith provision of telehealth using remote communication technologies
- Applies to telehealth provided for any reason (not limited to diagnosis & treatment of COVID-19)
- Covered providers may use popular communications apps, like FaceTime or Skype, to provide telehealth
- Public facing communication apps like Facebook Live, Twitch, and TikTok should not be used

<https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html>

Telehealth Remote Communications Guidance

- Clarifies how OCR is applying the Notification to support the good faith provision of telehealth
- Guidance includes:
 - What covered entities are included and excluded under the Notification?
 - Which parts of the HIPAA Rules are included in the Notification?
 - Does the Notification apply to violations of 42 CFR Part 2, the HHS regulation that protects the confidentiality of substance use disorder patient records?
 - Where can covered health care providers conduct telehealth?
 - What is a “non-public facing” remote communication product?

<https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf>

Guidance on Disclosures to Law Enforcement, Other First Responders, and Public Health Authorities

- Identifies existing HIPAA Privacy Rule permissions and provides examples of when a covered entity may disclose PHI about individuals, without their HIPAA authorization, including:
 - When the disclosure is needed to provide treatment
 - When the disclosure is required by law
 - To notify a public health authority to prevent or control the spread of disease
 - When first responders may be at risk of infection
 - To prevent or lessen a serious and imminent threat
- Reminds about the minimum necessary standard

<https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf>



Notification of Enforcement Discretion on BA Uses & Disclosures for Public Health and Health Oversight

- OCR will not impose HIPAA penalties against covered health care providers or their business associates for good faith uses and disclosures of PHI by business associates for public health and health oversight activities
- Issued to support Federal public health authorities and health oversight agencies, state and local health departments, and state emergency operations centers who need access to COVID-19 related data, including PHI
- The HIPAA Privacy Rule already permits covered entities to provide this data, and this enforcement discretion now permits business associates to also share this data without risk of a HIPAA penalty

<https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-hipaa.pdf>

Notification of Enforcement Discretion Regarding COVID-19 Community-Based Testing Sites (CBTS)

- OCR will not impose HIPAA penalties against covered health care providers and their business associates in connection with the good faith participation in the operation of a CBTS during the COVID-19 nationwide public health emergency
- The operation of a CBTS includes all activities that support the collection of specimens from individuals for COVID-19 testing
- Reasonable safeguards to protect PHI are encouraged
- Examples of entities and activities that are not covered by the Notification

<https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-community-based-testing-sites.pdf>

Guidance on Media and Film Crew Access to PHI

- Reminds covered health care providers that the COVID-19 public health emergency does not alter the HIPAA Privacy Rule restrictions on disclosures of PHI to the media
 - Written authorization from each patient whose PHI will be accessible to the media must be obtained *before* giving the media access to that patient's PHI
 - Masking or obscuring patients' faces before broadcasting a recording is not a sufficient alternative
 - In 2016 and 2018, OCR successfully resolved investigations about covered hospitals' unauthorized disclosures of patients' PHI to television film crews

<https://www.hhs.gov/sites/default/files/guidance-on-media-and-film-crews-access-to-phi.pdf>

Guidance on How CEs Can Contact Former COVID-19 Patients About Plasma Donation Opportunities

- HIPAA permits covered entities, including health plans, to identify and contact individuals who have recovered from COVID-19 to inform them about how they can donate their plasma to help treat other patients with COVID-19
- The communication to recovered individuals is not considered marketing if the covered entity does not receive any financial remuneration for making the communication
- A covered entity may not disclose individuals' PHI to a plasma donation center, for the center's own purposes, without the individuals' authorization

<https://www.hhs.gov/sites/default/files/guidance-on-hipaa-and-contacting-former-covid-19-patients-about-plasma-donation.pdf>

Guidance on HIPAA, Health Information Exchanges, and Disclosures of PHI for Public Health Purposes

- HIPAA permits covered entities and their business associates to use health information exchanges (HIEs) to disclose protected health information (PHI) for the public health activities of a public health authority (PHA)
- The guidance provides examples relevant to the COVID-19 public health emergency on how HIPAA permits covered entities and their business associates to disclose PHI to an HIE for reporting to a PHA that is engaged in public health activities

<https://www.hhs.gov/sites/default/files/hie-faqs.pdf>

Notification of Enforcement Discretion for Use of WBSAs When Scheduling COVID-19 Vaccination Appointments

- OCR will not impose penalties on covered health care providers or their business associates in connection with the good faith use of online or web-based scheduling applications (“WBSAs”) for scheduling of individual appointments for COVID-19 vaccinations during the COVID-19 nationwide public health emergency
- A WBSA is a non-public facing application that allows only the intended parties to access the data created, received, maintained, or transmitted by the WSA
- Reasonable safeguards to protect PHI are encouraged
- Effective immediately, but has retroactive effect to December 11, 2020

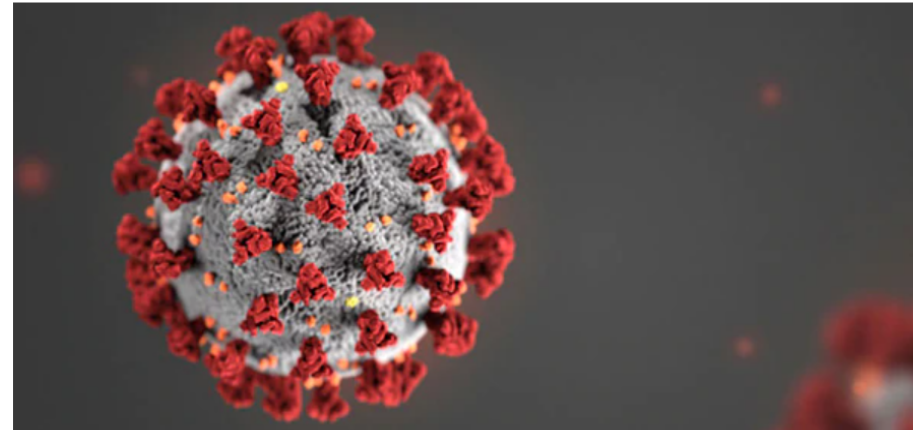
<https://www.hhs.gov/sites/default/files/hipaa-vaccine-ned.pdf>

HIPAA and COVID-19 Web Page



Regulatory Initiatives
Privacy +
Security +
Breach Notification +
Compliance & Enforcement +
Special Topics -
HIPAA and COVID-19
HIPAA and FERPA
Mental Health & Substance Use Disorders
Research
Public Health

HIPAA and COVID-19



The HHS Office for Civil Rights (OCR) has provided Bulletins, Notifications of Enforcement Discretion, Guidance, and Resources that help explain how patient health information may be used and disclosed in response to the COVID-19 nationwide public health emergency.

OCR HIPAA Announcements Related to COVID-19:

- [OCR Announces Notification of Enforcement Discretion for Use of Online or Web-Based Scheduling Applications for the Scheduling of COVID-19 Vaccination Appointments](#) – January 19, 2021

* OCR Notifications, Guidance, and Bulletins on HIPAA and COVID-19 are available in Spanish.



BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

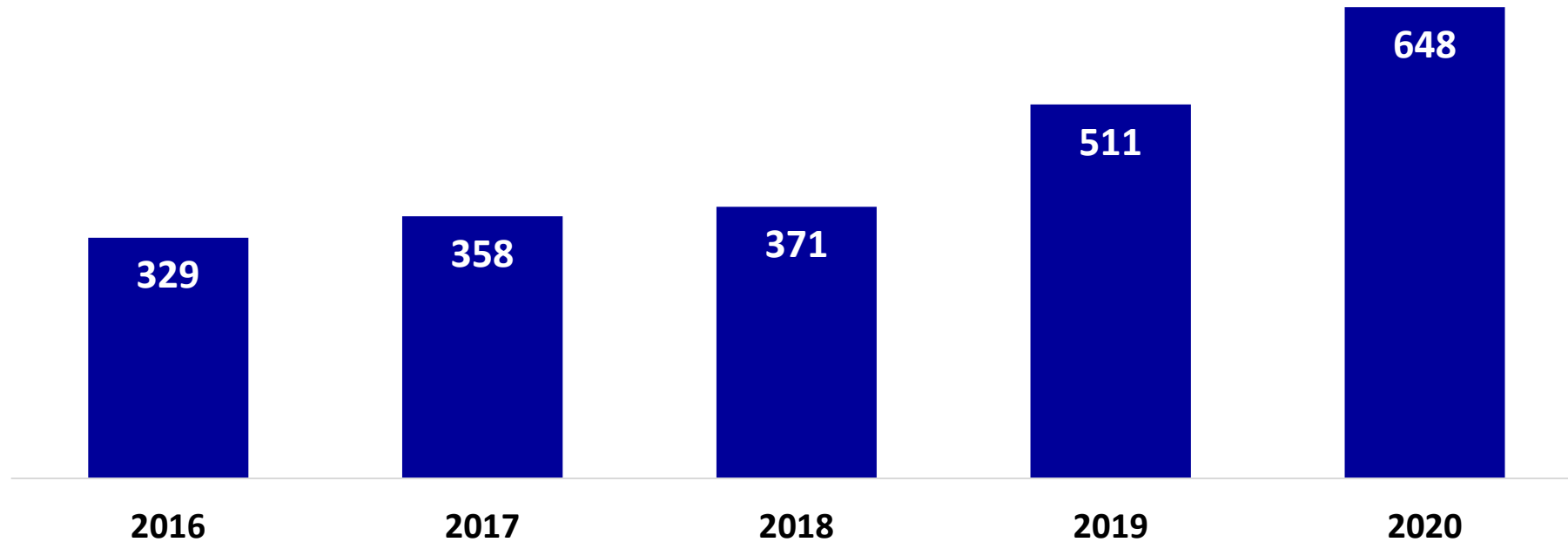


What Happens When OCR Receives a Breach Report

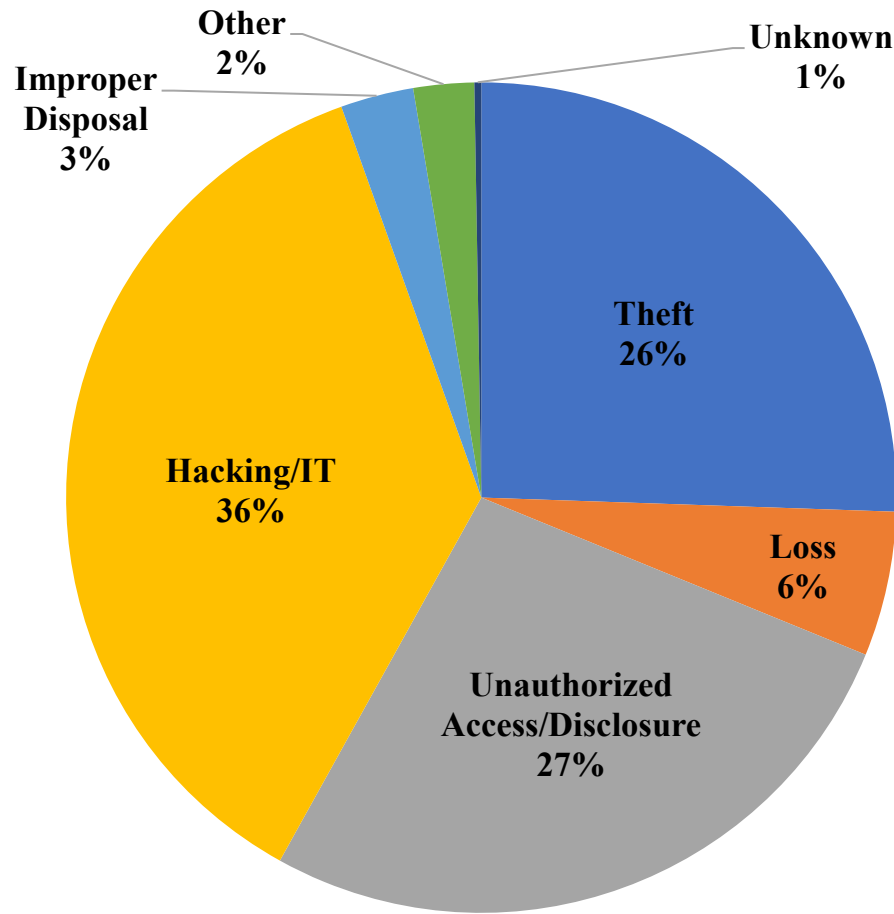
- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
 - Public can search and sort posted breaches
 - Received over 600 breach reports affecting 500+ individuals last year
- OCR opens investigations into breaches affecting 500+ individuals, and into a number of smaller breaches
- OCR breach investigations examine:
 - Underlying cause of the breach
 - Actions taken to respond to the breach (breach notification) and prevent future incidents
 - Entity's compliance prior to the breach

Breaches Affecting 500 or More Individuals Reports Received by Year

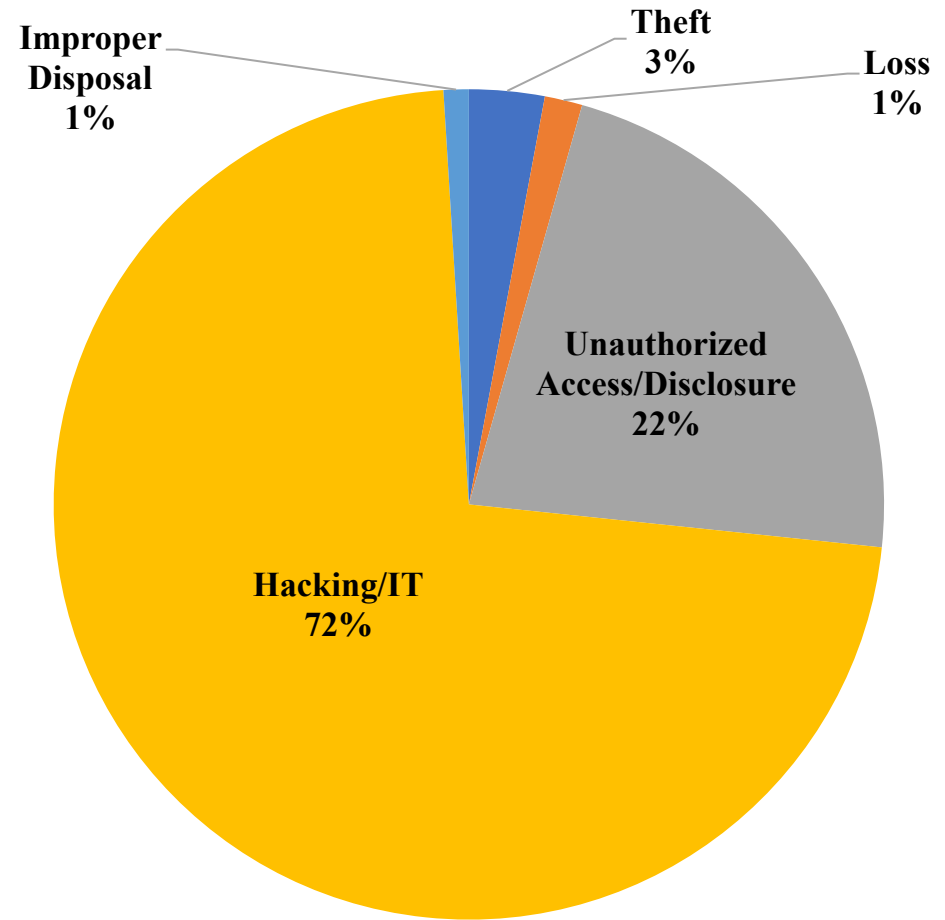
Calendar Years 2016 - 2020



500+ Breaches by Type of Breach



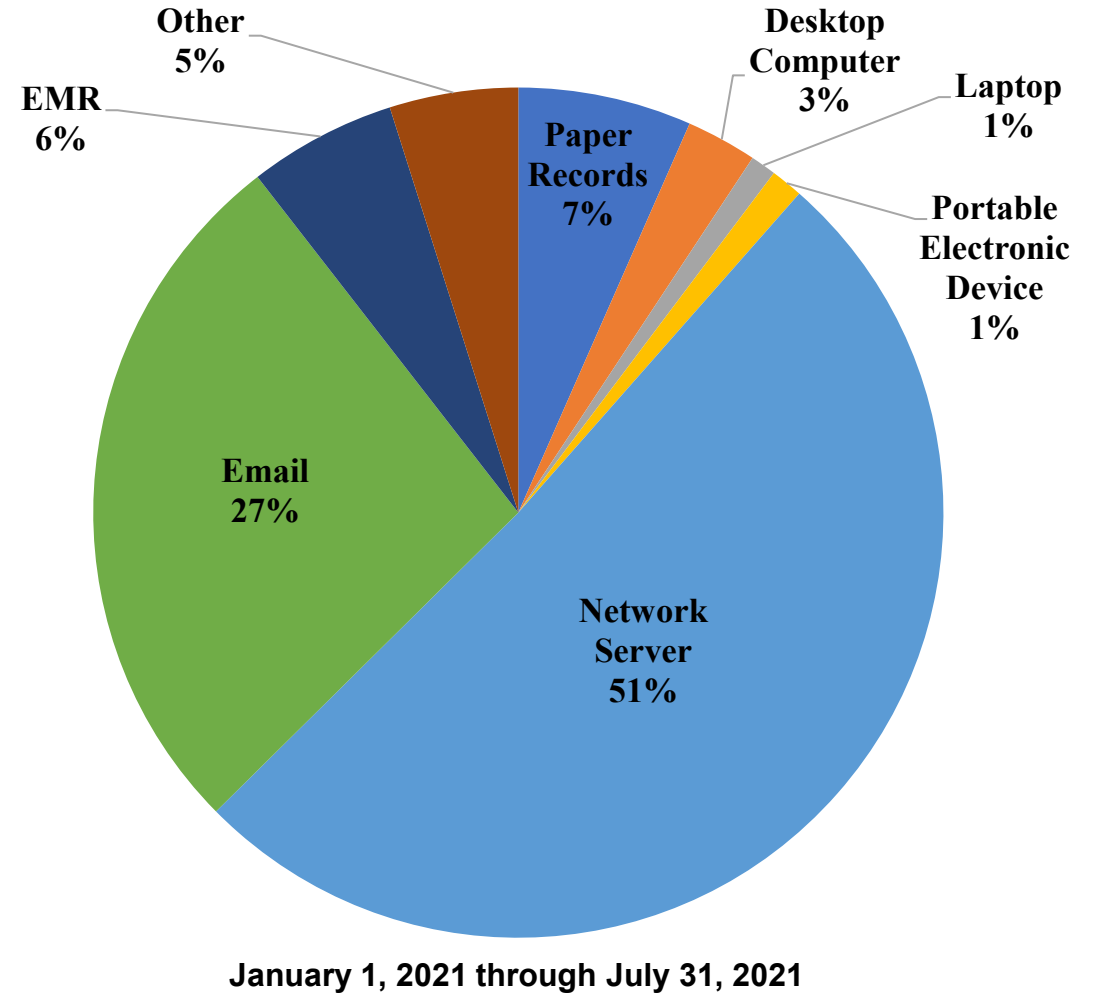
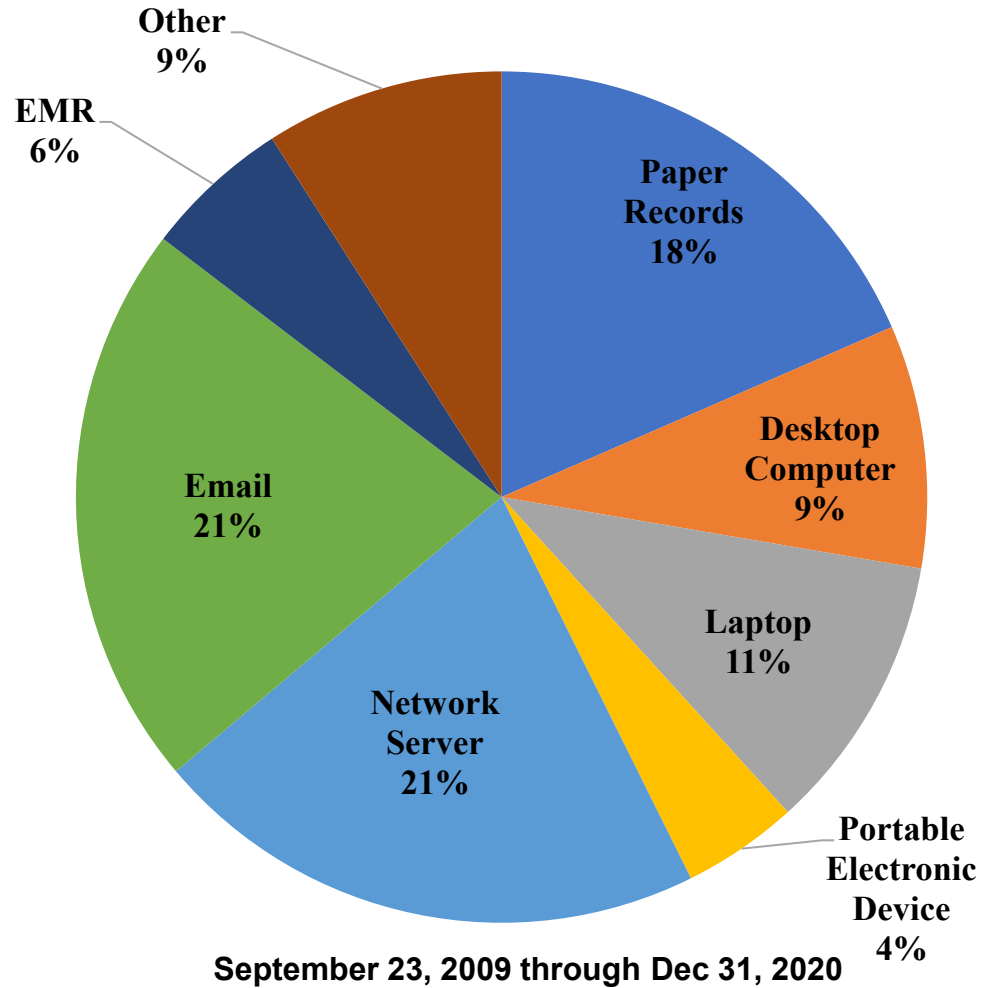
September 23, 2009 through Dec 31, 2020



January 1, 2021 through July 31, 2021

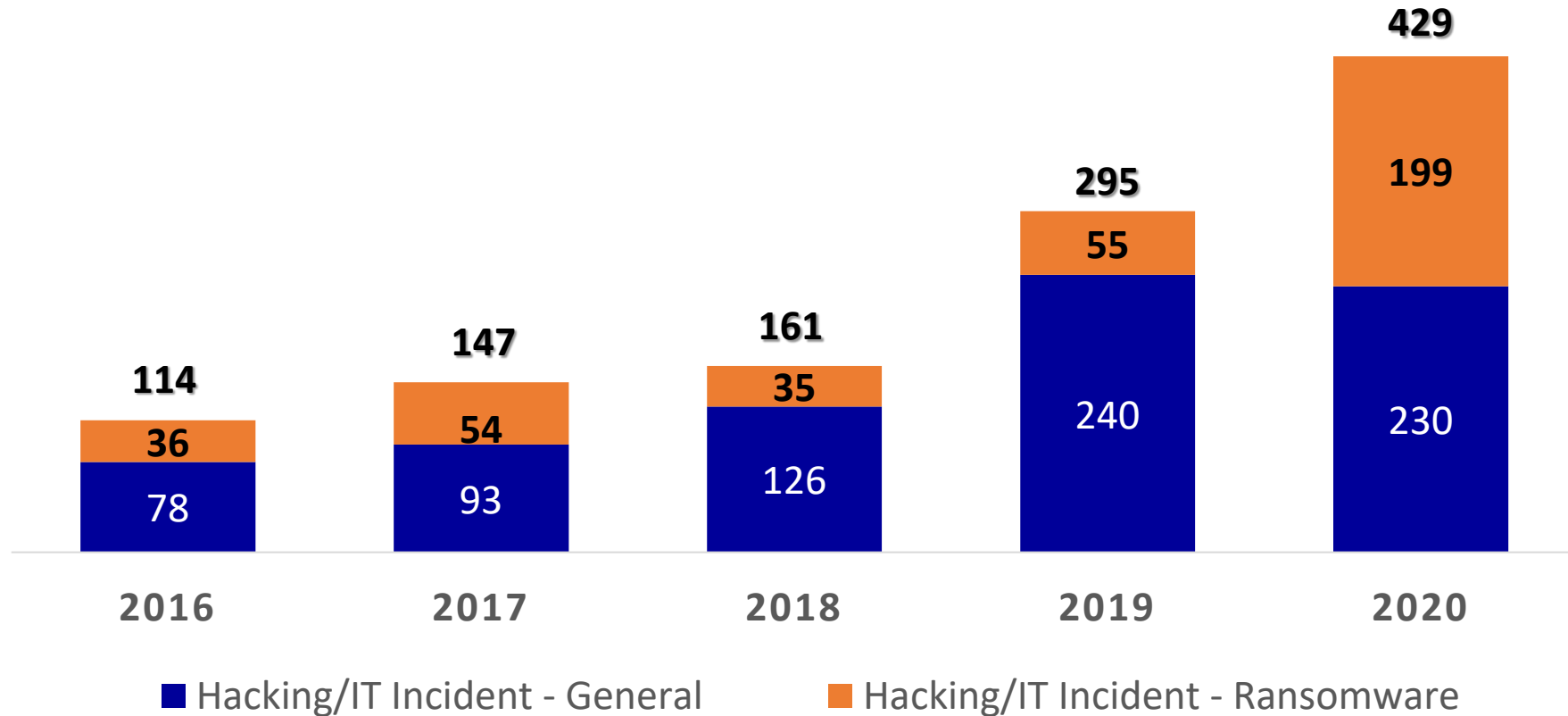


500+ Breaches by Location of Breach



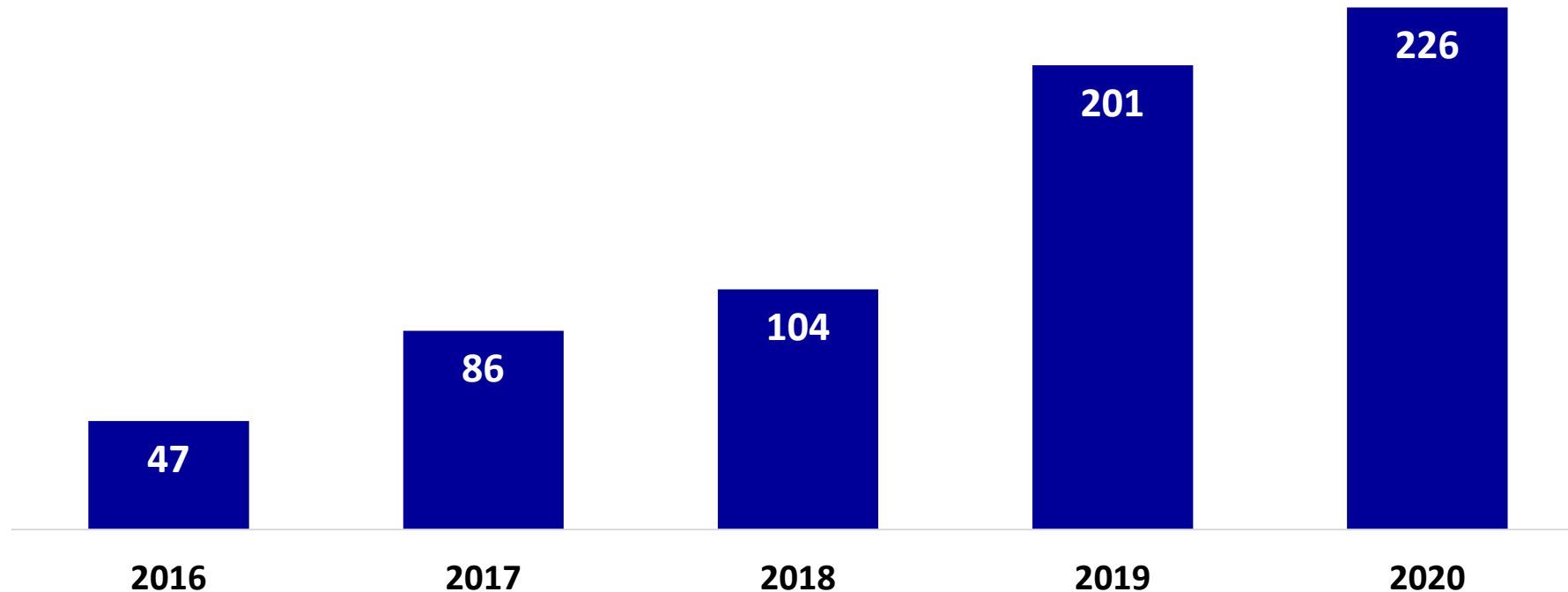
Breaches Affecting 500 or More Individuals Reports Received Involving Hacking/IT Incidents

Calendar Years 2016 - 2020



Breaches Affecting 500 or More Individuals Reports Received of Breaches Involving Email Accounts

Calendar Years 2016 - 2020



General HIPAA Enforcement Highlights

- OCR expects to receive over 28,000 complaints this year.
- In most cases, entities are able to demonstrate satisfactory compliance through voluntary cooperation and corrective action.
- In some cases, the nature or scope of indicated noncompliance warrants additional enforcement action.
- Resolution Agreements/Corrective Action Plans
 - 95 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 5 civil money penalties

As of July 31, 2021



Recent OCR HIPAA Enforcement Actions

Aug-20	Beth Israel Lahey Health Behavioral Services	\$70,000
Aug-20	King MD	\$3,500
Aug-20	Wise Psychiatry, PC	\$10,000
Sept-20	St. Joseph's Hospital and Medical Center	\$160,000
Sept-20	NY Spine Medicine	\$100,000
Oct-20	Aetna	\$1,000,000
Oct-20	City of New Haven, CT	\$202,400
Oct-20	Riverside Psychiatric Medical Group	\$25,000
Oct-20	Dr. Rajendra Bhayani	\$15,000
Nov-20	University of Cincinnati Medical Center	\$65,000
Dec-20	Elite Primary Care	\$36,000
Jan-21	Banner Health	\$200,000
Jan-21	Excellus	\$5,100,000
Feb-21	Renown Health	\$75,000
Feb-21	Sharp Healthcare	\$75,000
Mar-21	Arbour	\$65,000
Mar-21	Village Plastic Surgery	\$30,000
Apr-21	Peachstate	\$25,000
May-21	Diabetes, Endocrinology & Lipidology Center, Inc.	\$5,000

Right of Access Initiative

- Announced in February 2019
- Individuals have a right to timely access to their health records, and at a reasonable, cost-based fee
- Investigations launched across the country
- Nineteen settlements to date

Recurring HIPAA Compliance Issues

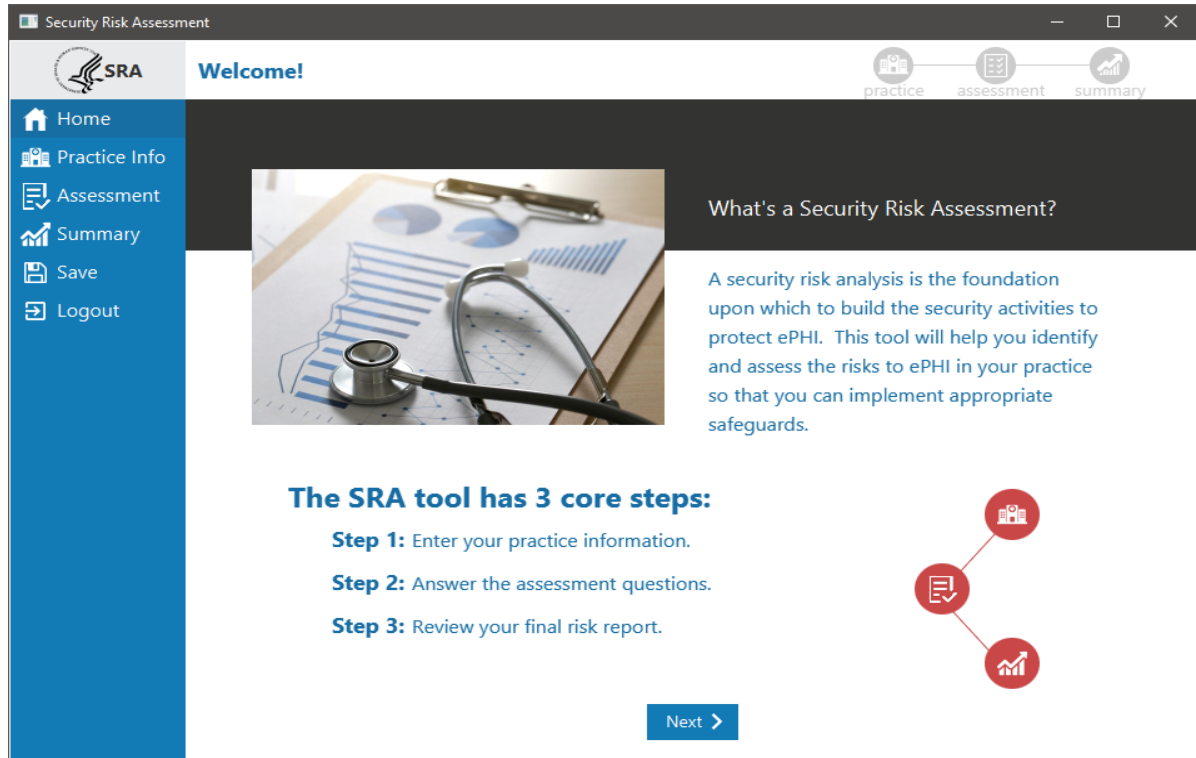
- Individual Right of Access
- Risk Analysis
- Business Associate Agreements
- Access Controls
- Audit Controls
- Information System Activity Review

Best Practices

Some Best Practices:

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security

SRA Tool



<https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>

Designed to assist small to medium sized organizations in conducting an internal security risk assessment to aid in meeting the security risk analysis requirements of the HIPAA Security Rule and the CMS EHR Incentive Program.

The SRA tool guides users through a series of questions based on standards identified in the HIPAA Security Rule. Responses are sorted into Areas of Success and Areas for Review.

Not all areas of risk may be captured by the tool. Risks not identified and assessed via the SRA Tool must be documented elsewhere.

Cybersecurity Newsletters

- Recent Topics Include:
 - Controlling Access to ePHI
 - HIPAA and IT Asset Inventories
 - Preventing, Mitigating, and Responding to Ransomware
 - Advanced Persistent Threats and Zero Day Vulnerabilities
 - Managing Malicious Insider Threats
 - Phishing
 - Software Vulnerabilities and Patching
 - Securing Electronic Media and Devices
- Sign up for the OCR Listserv:
<http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>





Connect with Us

Office for Civil Rights

U.S. Department of Health and Human Services



www.hhs.gov/hipaa



Join our Privacy and Security listservs at

<https://www.hhs.gov/hipaa/for-professionals/list-serve/>



@HHSOCR



Contact Us

Office for Civil Rights

U.S. Department of Health and Human Services



ocrmail@hhs.gov

www.hhs.gov/ocr



Voice: (800) 368-1019

TDD: (800) 537-7697

Fax: (202) 519-3818



200 Independence Avenue, S.W.

H.H.H Building, Room 509-F

Washington, D.C. 20201

UNITED STATES

Department of
Health and Human
Services



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights