MEDICUS IT

We do 'IT' Right!

Healthcare IT Risks and Recommendations As Practices Resume Operations

www.medicusit.com

Meet Today's Speaker

Nelson Gomes
NJ President, Senior Vice President
of Development, Medicus IT

Program Overview

- Understanding the latest security threats, vulnerabilities, and exploits
- Expanding security policies with best practices
- Achieving the right balance between security and usability
- Appreciating the importance of taking a zero-trust approach
- Making infrastructure and equipment decisions today to succeed tomorrow
- Strengthening continuity planning
- Avoiding HIPAA and other regulatory missteps
- Your questions

Security Threats, Vulnerabilities, and Exploits

- What are the bad guys thinking
- What are the bad guys doing
- How are the bad guys targeting

Security Threats, Vulnerabilities, and Exploits

Security Threats, Vulnerabilities, and Exploits

THE UNITED STATES DEPARTMENT of JUSTICE

Search this site

ABOUT OUR AGENCY PRIORITIES NEWS RESOURCES CAREERS CONTACT

Office of Public Affairs

FOR IMMEDIATE RELEASE

Friday, March 20, 2020

Attorney General William P. Barr Urges American Public to Report COVID-19 Fraud

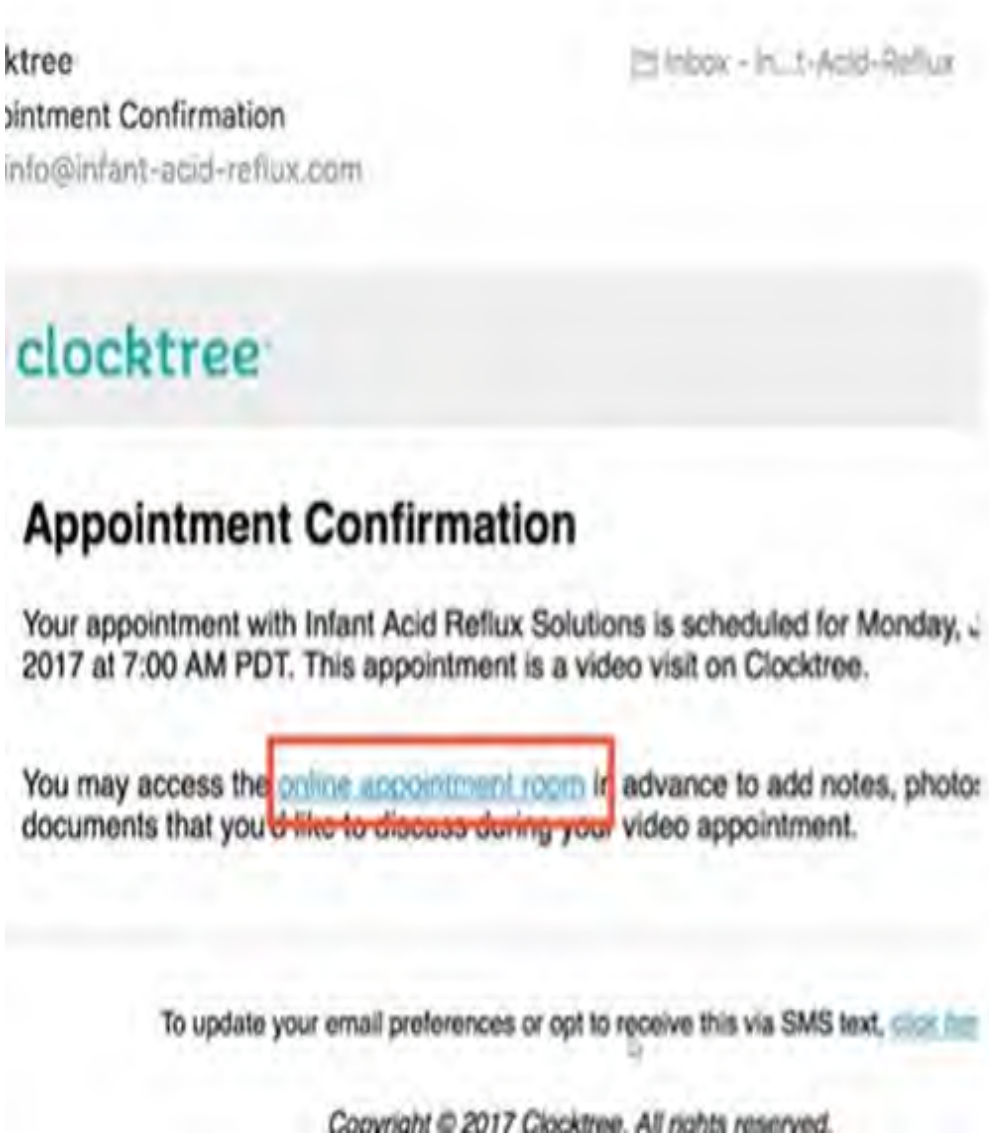
Attorney General William P. Barr is urging the public to report suspected fraud schemes related to COVID-19 (the Coronavirus) by calling the National Center for Disaster Fraud (NCDF) hotline (1-866-720-5721) or by e-mailing the NCDF at disaster@leo.gov.

This week, Attorney General Barr directed all U.S. Attorneys to prioritize the investigation and prosecution of Coronavirus-related fraud schemes. In a follow-up memorandum issued March 19, Deputy Attorney General Jeffrey Rosen further directed each U.S. Attorney to appoint a Coronavirus Fraud Coordinator to serve as the legal counsel for the federal judicial district on matters relating to the Coronavirus, direct the prosecution of Coronavirus-related crimes, and to conduct outreach and awareness.

Some examples of these schemes include:

- Individuals and businesses selling fake cures for COVID-19 online and engaging in other forms of fraud.
- **Phishing emails from entities posing as the World Health Organization or the Centers for Disease Control and Prevention.**
- Malicious websites and apps that appear to share Coronavirus-related information to gain and lock access to your devices until payment is received.
- Seeking donations fraudulently for illegitimate or non-existent charitable organizations.
- Medical providers obtaining patient information for COVID-19 testing and then using that information to fraudulently bill for other tests and procedures.

Security Threats, Vulnerabilities, and Exploits



ktree
intment Confirmation
info@infant-acid-reflux.com

Inbox - In...t-Acid-Reflux

clocktree

Appointment Confirmation

Your appointment with Infant Acid Reflux Solutions is scheduled for Monday, ..
2017 at 7:00 AM PDT. This appointment is a video visit on Clocktree.

You may access the online appointment room in advance to add notes, photos
documents that you'd like to discuss during your video appointment.

To update your email preferences or opt to receive this via SMS text, click here

Copyright © 2017 Clocktree. All rights reserved.

dr chrono

John,

Your video visit appointment has been created!

You are scheduled for a video visit appointment with Dr. Khan on *Monday, October 10th at 10:00 AM PDT.*

Please sign in to verify your insurance and contact information.

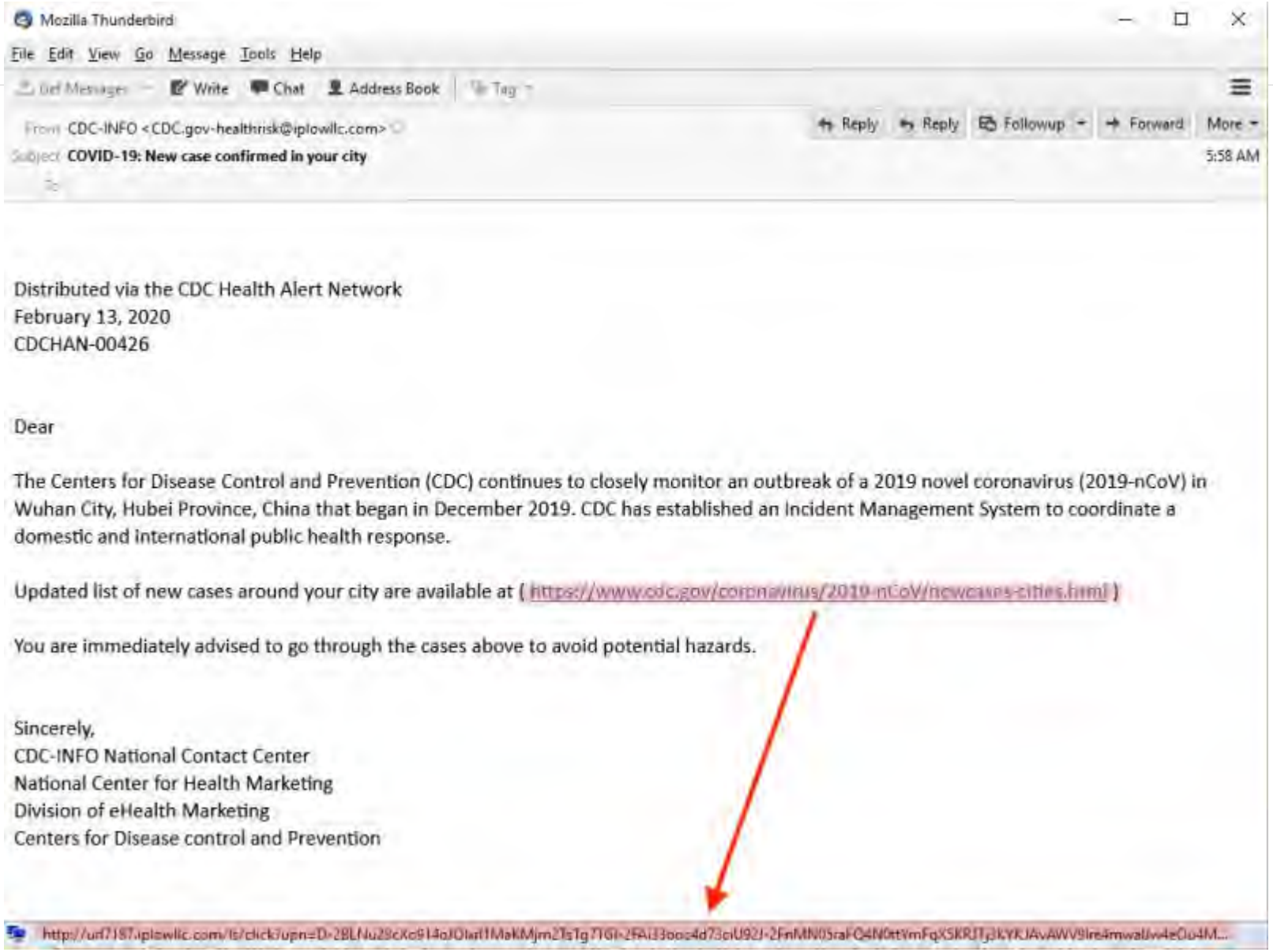
Sign In Now >>

Video visits are easy and convenient. Less time in the doctor's office means more time back in your day. Ditch the drive, see your doctor over video!

Best,

Chiron Health Video Visit Team

Phishing Email COVID-19 Targeting



Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

From CDC-INFO <CDC.gov-healthrisk@iplowllc.com>

Subject **COVID-19: New case confirmed in your city**

Reply Reply Followup Forward More

5:58 AM

Distributed via the CDC Health Alert Network
February 13, 2020
CDCHAN-00426

Dear

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

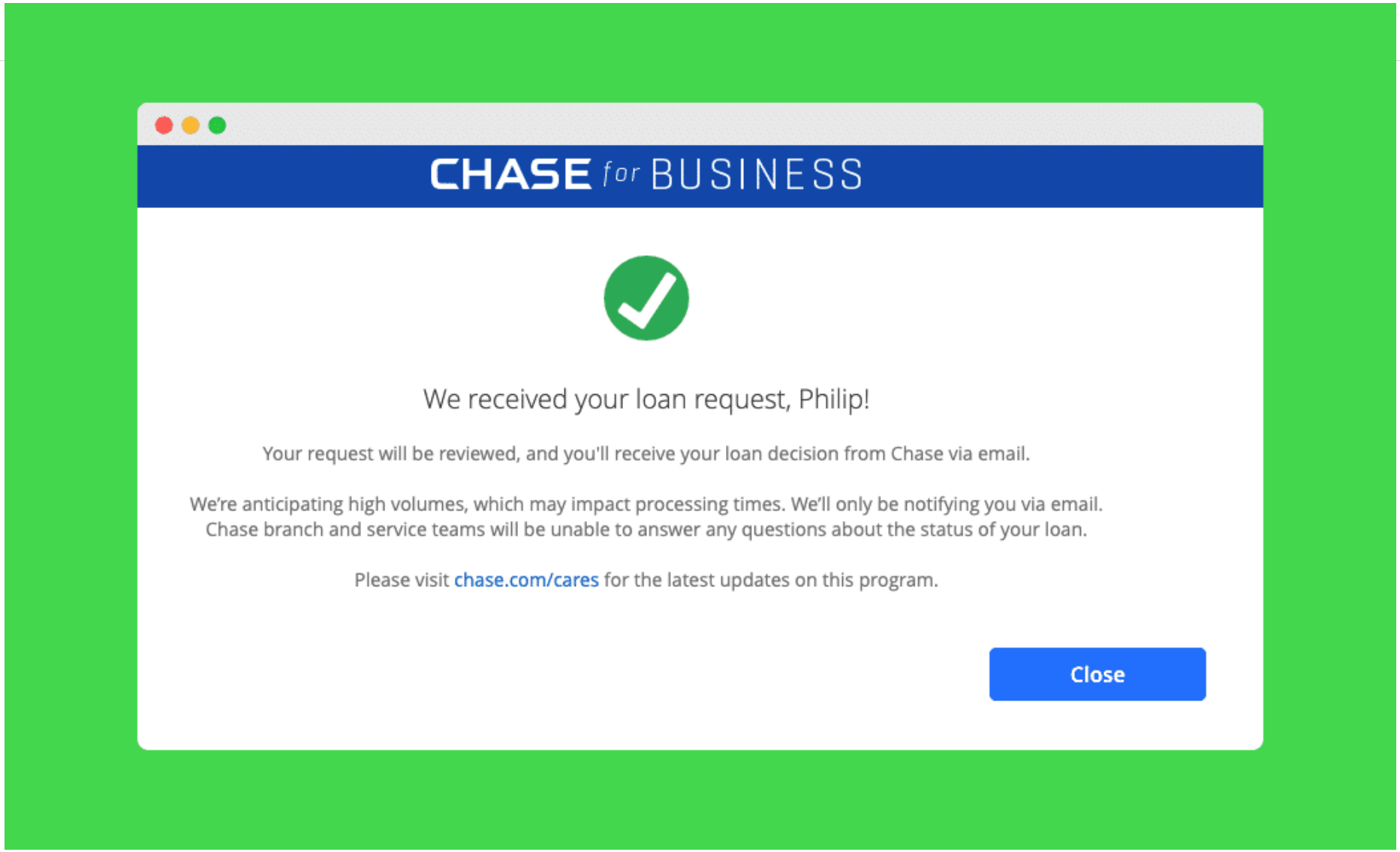
Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

http://url7187.iplowllc.com/ls/click?upn=D-2BLNu29cXc9I4oJOiaf1MaKMjm2TsTg7IGi-2FAi33ooc4d73oU92J-2FnMN05raFQ4N0ttYmFqXSKRJTj3KYKJAvAWV9Ire4mwaUw4eOo4M...

Phishing PPP Loan Targeting

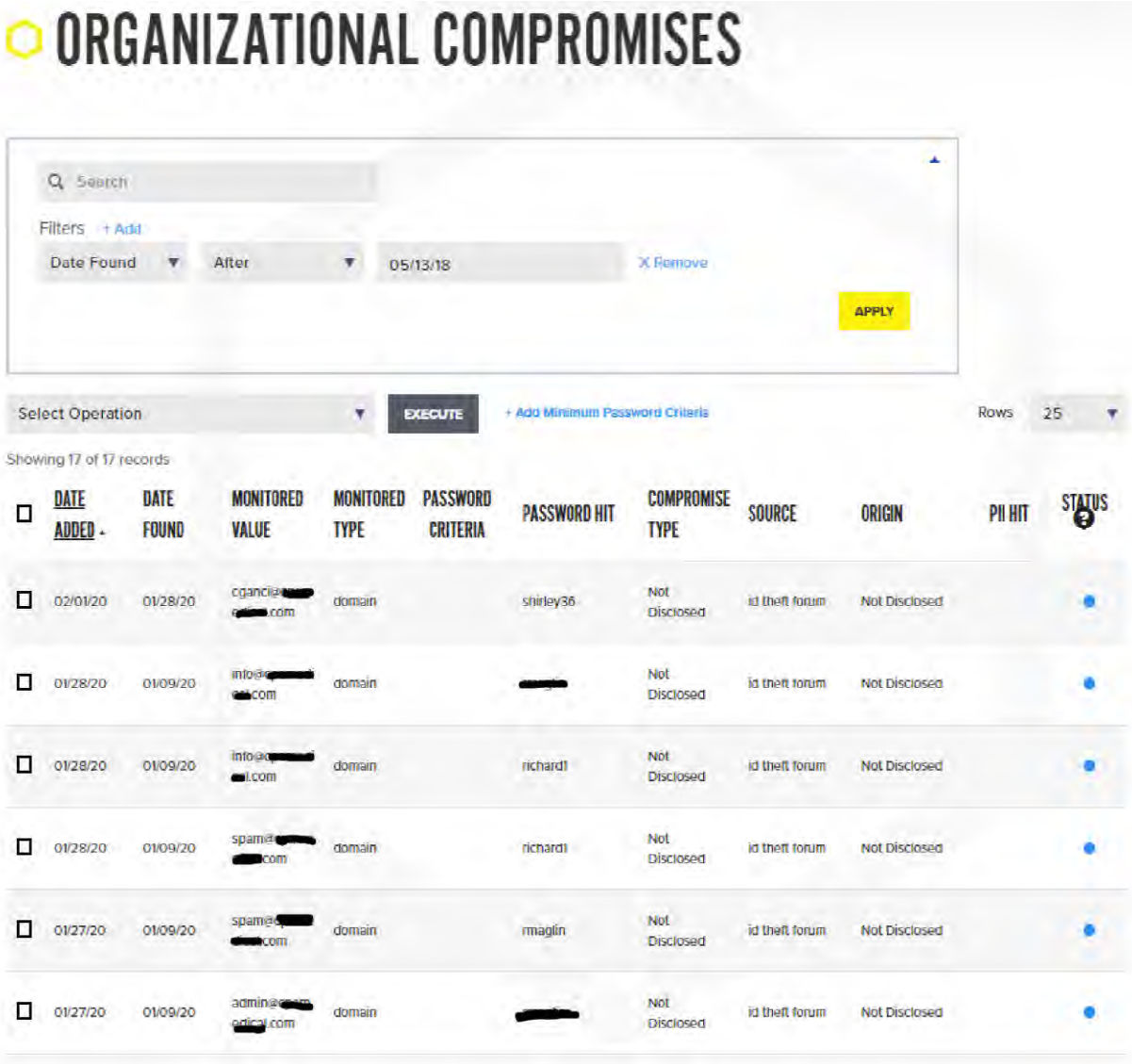


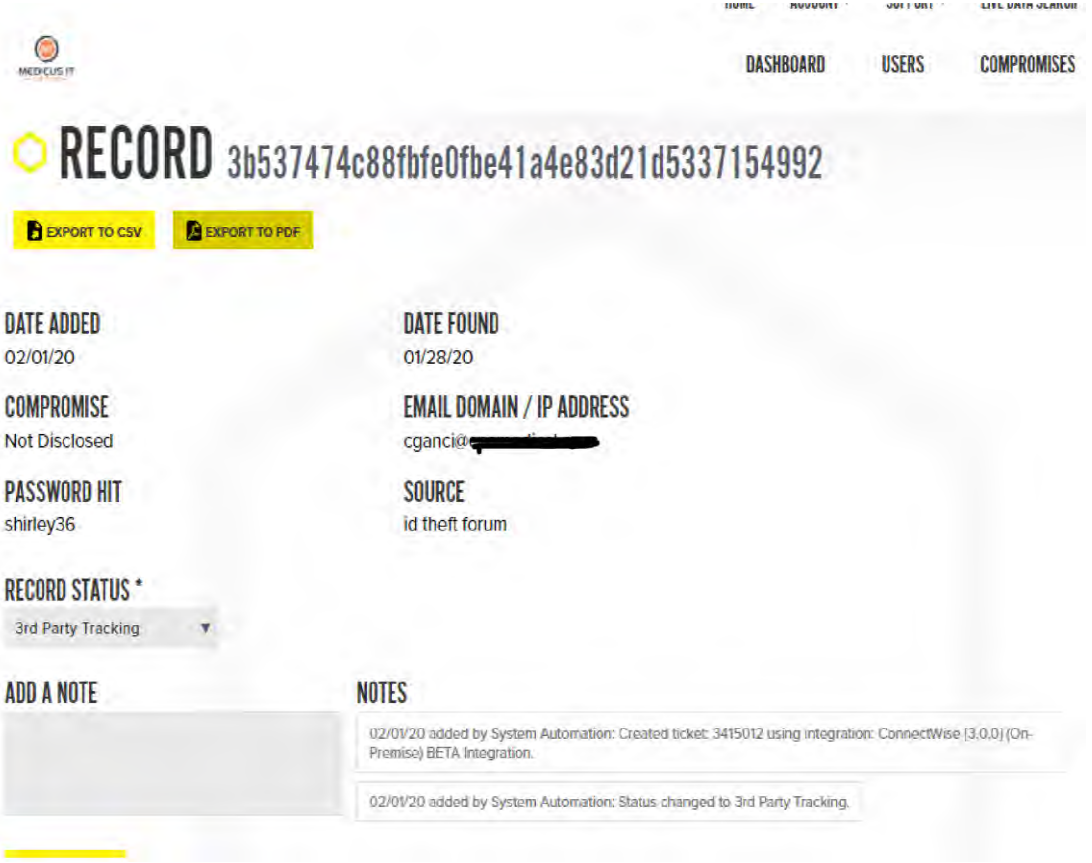
Phishing Amazon Targeting

Understanding Security Policies with Best Practices

- Dark Web Scans
- 2/MFA Multi Factor Authentication
- Encryption
- Training Staff

Dark Web Scan





Multi-Factor Authentication

What is Zero Trust and Why Is it So Important?

1. Verify Every User

2. Validate Their Devices

3. Intelligently Limit Their Access

info@medicusit.com #WeAreMedicusIT

MEDICUS IT
We do 'IT' Right!

Making Infrastructure and Equipment Decisions

- Infection control technology
  - Keyboards
  - Mice
  - UV-C disinfection systems (cellphones, tablets)
- A good time to consider working on IT projects
  - System upgrades
  - Equipment refresh
- Revisit internet connectivity
- VOIP phone systems
- Wireless network and guest access
- Collaboration solutions

Strengthening Continuity Planning

- Develop a *Business Impact Analysis*. Focus on the following perspectives:
  - People
  - Process
  - Technology
- Business Continuity Planning
- Disaster Recovery
- Testing
- Revisit Continuity and Disaster Recovery Plans
- Rinse and Repeat

Strengthening Continuity Planning

- What you need to consider to be part of the continuity plan:
  - Work from home policy
  - VOIP phone system that have softphone capabilities
  - Secure connectivity to mission critical applications with 2MFA
  - Collaboration solutions
    - Microsoft Teams
    - Zoom

QUESTIONS ?

Nelson Gomes
SVP Business Development
ngomes@medicusit.com
201.505.1800 ext 2001

GARFUNKEL WILD, P.C.
ATTORNEYS AT LAW

Healthcare IT Risks and Recommendations As Practices Resume Operations

Stacey L. Gulick, Esq.
Garfunkel Wild, P.C.

516-393-2264
Sgulick@garfunkelwild.com

COVID WAIVERS

As a result of the Coronavirus pandemic/public health emergency, the OCR announced easing of the HIPAA requirements to allow for greater response to the pandemic, including waiver of potential HIPAA penalties in connection with:

- use of everyday communications technologies (i.e., telehealth). This exercise of discretion applies to widely available communications apps, such as FaceTime or Skype, when used in good faith for any telehealth treatment or diagnostic purpose, **regardless of whether the telehealth service is directly related to COVID-19.**
- the good faith participation in the operation of COVID-19 testing sites during the COVID-19 nationwide public health emergency.
- the good faith uses and disclosures of PHI by business associates for public health and health oversight activities during the COVID-19 nationwide public health emergency.

COVID GUIDANCE

During the COVID pandemic, OCR also clarified HIPAA rules to allow for:

- Ease of communications with Emergency Response personnel.
- Communication with COVID positive patients regarding blood and plasma donation; however, without patients' authorization, the providers cannot receive any payment from or on behalf of a blood and plasma donation center in exchange for such communications with recovered patients.

BUT ENFORCEMENT DID NOT STOP

- Continued emphasis on the need to encrypt mobile devices.
- Increased enforcement of patient access requirements.
- Focus on importance of terminating access when employment ends.
- Compliance with HIPAA Breach Notification requirements.
- Concern with requirements for media access.
- Continued emphasis on paper mailings that disclose PHI to the public.
- Review of hacking events that lead to Breaches.

MEDIA ACCESS

- Amidst the pandemic, providers, particularly hospitals began to allow the media access to publicize the extent of the crisis. The OCR criticized providers for even allowing access to patients without a patient authorization.
- OCR issues guidance in May 2020 which states that even during the current COVID-19 public health emergency, covered health care providers are still required to obtain a valid HIPAA authorization from each patient **before** the media is given access to that PHI. Masking or obscuring patients' faces or identifying information before broadcasting a recording of a patient is not sufficient, as a valid HIPAA authorization is still required before giving the media such access.

"The last thing hospital patients need to worry about during the COVID-19 crisis is a film crew walking around their bed shooting 'B-roll,'" said Roger Severino, OCR Director. "Hospitals and health care providers must get authorization from patients before giving the media access to their medical information; obscuring faces after the fact just doesn't cut it," Severino added.

SETTLEMENTS

WHO HAS TO BE NOTIFIED?

It was announced November 17, 2019 that Sentara Hospitals (Sentara) agreed to pay $2.175 million to settle potential violations of HIPAA Breach Notification and Privacy Rules. Sentara is comprised of 12 acute care hospitals with more than 300 sites of care throughout Virginia and North Carolina.

In April of 2017, HHS received a complaint alleging that Sentara had sent a bill to an individual containing another patient's PHI. OCR's investigation determined that Sentara mailed 577 patients' PHI to wrong addresses that included patient names, account numbers, and dates of services. Sentara reported this incident as a breach affecting 8 individuals, because Sentara concluded, **incorrectly**, that unless the disclosure included patient diagnosis, treatment information or other medical information, no reportable breach of PHI had occurred. Sentara persisted in its refusal to properly report the breach even after being explicitly advised of their duty to do so by OCR. OCR also determined that Sentara failed to have a business associate agreement in place with Sentara Healthcare, an entity that performed business associate services for Sentara

FAILURE TO TERMINATE

The City of New Haven, agreed to pay $202,400 to OCR and to settle potential violations of the Privacy and Security Rules. In January 2017, New Haven filed a breach report stating that a former employee accessed a file on a New Haven computer containing the PHI of 498 individuals. OCR's investigation revealed that, on July 27, 2016, a former employee returned to New Haven, eight days after being terminated, logged into her old computer with her still-active user name and password, and downloaded PHI that included patient names, addresses, dates of birth and sexually transmitted disease test results onto a USB drive. Additionally, OCR found that the former employee had shared her user ID and password with an intern, who continued to use these login credentials to access PHI on New Haven's network after the employee was terminated.

MD COMPLAINT LEADS TO PENALTIES

The practice of Steven A. Porter, M.D., has agreed to pay $100,000 for HIPAA violations after complaining about EHR vendor. OCR initiated a compliance review of the Practice following the receipt of the Practice's breach report in November 2013. The Practice's breach report claimed that Elevation43, a business associate of Dr. Porter's EHR company, was impermissibly using the Practice's ePHI by blocking the Practice's access to such ePHI until Dr. Porter paid Elevation43 $50,000. OCR's investigation of the Practice revealed that the Practice demonstrated significant noncompliance with the HIPAA Rules, including:

- Failure to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of all its ePHI.
- Failure to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
- Permitting Dr. Porter's EHR company to create, receive, maintain, or transmit ePHI on the Practice's behalf at least since 2013 without obtaining satisfactory assurances that the EHR company will appropriately safeguard the ePHI.

HACKERS

- Athens Orthopedic Clinic PA ("Athens Orthopedic") agreed to pay $1.5m to address potential HIPAA violations. On June 26, 2016, a journalist notified Athens Orthopedic that a database of their patient records may have been posted online for sale. On June 28, 2016, a hacker contacted Athens Orthopedic and demanded money in return for a complete copy of the database. The hacker used a vendor's credentials on June 14, 2016, to access the EHR and exfiltrate patient health data. The hacker continued to access PHI for over a month until July 16, 2016. 208,557 individuals were affected by this breach, and the PHI included patients' names, dates of birth, SSN, medical procedures, test results, and health insurance information.
- OCR's investigation discovered longstanding, systemic noncompliance with HIPAA by Athens Orthopedic including failures to conduct a risk analysis, implement risk management and audit controls, maintain HIPAA policies and procedures, secure business associate agreements with multiple business associates, and provide HIPAA Privacy Rule training to workforce members.

MULTIPLE BREACHES

Aetna agreed to pay $1m to settle potential violations of HIPAA following disclosure of three (3) breaches in 2017:

- 2 web services allowed PHI to be accessible without login credentials and subsequently indexed by various internet search engines. 5,002 individuals were affected by this breach.
- Benefit notices were mailed to members using window envelopes. The words "HIV medication" could be seen through the envelope's window. Aetna reported that 11,887 individuals were affected by this impermissible disclosure.
- A research study mailing sent to Aetna plan members contained the name and logo of the atrial fibrillation (irregular heartbeat) research study in which they were participating, on the envelope. Aetna reported that 1,600 individuals were affected by this impermissible disclosure.

OCR's investigation revealed that in addition to the impermissible disclosures, Aetna failed to perform evaluations of the security of their ePHI; implement procedures to verify the identity of persons seeking access to ePHI; limit PHI disclosures to the minimum necessary; and have in place appropriate safeguards to protect PHI.

ENCRYPTION – A MUST

The University of Rochester Medical Center (URMC) agreed to pay **$3 million** to settle potential violations of HIPAA. URMC filed breach reports with OCR in 2013 and 2017 following its discovery that PHI had been impermissibly disclosed through the loss of an unencrypted flash drive and theft of an unencrypted laptop, respectively. OCR's investigation revealed that URMC failed to conduct an enterprise-wide risk analysis; implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; utilize device and media controls; and employ a mechanism to encrypt and decrypt ePHI when it was reasonable and appropriate to do so. Of note, in 2010, OCR investigated URMC concerning a similar breach involving a lost unencrypted flash drive and provided technical assistance to URMC. Despite the previous OCR investigation, and URMC's own identification of a lack of encryption as a high risk to ePHI, URMC permitted the continued use of unencrypted mobile devices.

AND – AGAIN – ENCRYPTION

- Lifespan Health System Affiliated Covered Entity (Lifespan ACE), a health system based in Rhode Island, has agreed to pay **$1.4m** to settle potential violations of HIPAA related to the theft of an unencrypted laptop. On April 21, 2017, Lifespan Corporation, the parent company and business associate of Lifespan ACE, filed a breach report with OCR concerning the theft of an affiliated hospital employee's laptop containing ePHI including: patients' names, medical record numbers, demographic information, and medication information. The breach affected 20,431 individuals.
- OCR's investigation determined that there was systemic noncompliance with the HIPAA Rules including a failure to encrypt ePHI on laptops after Lifespan ACE determined it was reasonable and appropriate to do so. OCR also uncovered a lack of device and media controls, and a failure to have a business associate agreement in place with the Lifespan Corporation.

10 SETTLEMENTS

In the past year the OCR has announced ten settlements involving covered entities failing to grant patients' timely access to their medical records. The settlement amounts range from $3500 to $160,000 and in each instance involve only one patient complaint. The OCR confirmed in its press releases that these settlements are intended to send a strong message to providers that they need to ensure that patients are provided timely and complete access to their medical records.

PATIENT ACCESS ENFORCEMENT DURING PANDEMIC

- Saint Joseph's Hospital and Medical Center (Phoenix, AZ) paid $160,000 because the mother of patient waited over 22 months to receive a complete copy of her son's medical records (and only received the missing portions after she complained to the OCR). A portion of the medical record was provided in a timely manner, but the mother's subsequent requests were ignored.
- NY Spine Medicine (New York City, NY) paid $100,000 because one patient waited over a year to receive copies of her diagnostic films (and only received films after she complained to the OCR). The rest of her medical record had been provided in a timely manner.
- Housing Works, Inc (New York City, NY) paid $38,000, King MD (Virginia) paid $3500 and Wise Psychiatry, PC (Colorado) paid $10,000 after each failed to provide medical records after receiving instructions from the OCR to provide the records. In each instance, the medical records were not provided until there was a second complaint to the OCR

PATIENT ACCESS ENFORCEMENT DURING PANDEMIC

- All Inclusive Medical Services, Inc. (Carmichael, CA) paid $15,000 after it failed to provide medical records to a patient until she complained to OCR.
- Beth Israel Lahey Health Behavioral Services (Eastern Massachusetts) paid $70,000 after it failed to provide a patient's personal representative with a copy of her father's medical records until the patient complained to the OCR.
- Riverside Psychiatric Medical Group paid $25,000 after it failed to provide patient access after multiple requests from patient and instructions from OCR to provide access. The Practice tried to argue that because there were psychotherapy notes, no information had to be provided.

ENSURING ONGOING HIPAA COMPLIANCE

HOW TO ENSURE COMPLIANCE DURING THE MAYHEM

- Continue to conduct routine comprehensive security risk analyses and prepare risk management plans.
- Do not allow the media access to any patients unless a HIPAA authorization is signed.
- Now that you have more time, find a telehealth platform that will provide assurances that the platform has the necessary safeguards to comply with HIPAA.
- Brush off you Patient Access policies and make sure that staff are aware of the requirements.
- Send out email blasts about new viruses and reminders about potential phishing attacks (and maintain copies of such communications)

HOW TO ENSURE COMPLIANCE DURING THE MAYHEM

- Ensure that you are aware of your Breach Notification requirements and get legal/technical guidance if you think that you had a significant breach.
- Install encryption on ALL portable devices that contain PHI.
- Purchase Cyberliability Insurance!!!!

AND MORE FUN ….
INFORMATION BLOCKING

INFORMATION BLOCKING

Implementation of Information Blocking Rules under the CURES Act has been postponed until April 2021!!!!

WHAT IS THAT?

The Information Blocking Rule applies to most healthcare providers as well as certain health technology vendors ("Affected Entities") and prohibits **interference with** access to, or exchange of, electronic health information ("EHI"). This is especially challenging for providers who will need to meet two objectives: (1) continue to protect EHI, as required by HIPAA and other existing laws, and (2) ensure that patients and others are provided timely access to such information.

PATIENT PORTAL

The Information Blocking Rules do not require providers to have a patient portal, but it makes compliance much easier …

INFORMATION INVOLVED

Initially, the Information Blocking Rule will restrict information blocking with respect to the elements of a USCDI data set (U.S. Core Data for Interoperability):

- Allergies & intolerances
- Assessment & plan of treatment
- Care team members
- Clinical notes
- Goals
- Health concerns
- Immunizations
- Laboratory tests and results
- Medications
- Patient demographics
- Problems
- Procedures
- Provenance
- Smoking status
- Unique device identifier for implantable device
- Vital signs

EXAMPLES

Examples of Potential Information Blocking include:

- Charging medical record access fees that are too high, or including inappropriate cost elements in the fee calculation.
- Failing to provide ALL information required by the rule in an EHR portal. For example, clinical notes will need to be provided without undue delay.
- Withholding an entire record when just a portion of the record may legitimately be withheld (e.g. substance abuse or psychotherapy notes).
- Withholding records or imported data that might theoretically contain errors, without actually verifying and documenting the impact and scope of actual inaccuracies or errors in the data.

EXAMPLES

- Delaying the publication of lab results to the portal until the patient makes an appointment to review them with a doctor, on the basis of a nebulous “harm to patient” justification.
- Requiring onerous identity-verification procedures before obtaining access to medical records (e.g., must come by the offices in person to request access).
- Restricting third parties from connecting into the EHR system, using a blanket excuse that any third party access might post an IT security risk.
- Taking the EHR system down for maintenance that takes too long to fix relative to the actual underlying problem.
- Claiming that information resides in a legacy system and therefore can’t be provided in the EHR portal.

EXCEPTIONS

There are a number of exceptions that function as safe harbors for certain practices. For example, providers cannot be required to disclose EHI if such disclosure is prohibited by law. Other exceptions focus on areas such as privacy rights, security requirements and protecting patients from harm. These safe harbors can be useful in operationalizing the Information Blocking Rule.

EXCEPTIONS

(1) Preventing Harm. The provider must have a reasonable belief that limited and tailored interference with EHI is necessary to substantially reduce risk of harm to a patient. The standard for patient harm is "reasonably likely to endanger the life or physical safety" of the patient.

(2) Privacy. Interference is permitted on privacy grounds, including: a precondition under State or Federal law to access the information was not satisfied, an unreviewable grounds for denial or if requested by a party other than the patient, respecting the patient's request not to share information.

(3) Security. A provider may engage in tailored, consistent and non-discriminatory practices directed to safeguarding the confidentiality, integrity, and availability of EHI. This may be according to a written organizational security policy or, if there is no such policy, a particularized determination that the practice is necessary and there is no reasonable and appropriate alternative.

EXCEPTIONS

(4) Infeasibility.

(5) Health IT Performance. This Exception permits temporary unavailability for maintenance and improvements, so long as the unavailability is tailored, consistent and non-discriminatory.

(6) Content and Manner. A provider must fulfill an EHI request in the manner requested, unless technically unable to do so or the provider cannot reach agreeable terms with the requestor.

(7) Fees. A provider may charge fees based on objective and uniformly applied criteria that are reasonably related to a provider's costs in fulfilling the EHI request. The fee must be allocated among similarly situated persons.

(8) Licensing. N/A

PENALTIES

Affected Entities that violate the Information Blocking Rule by engaging in prohibited information blocking practices will be subject to monetary penalties or other "disincentives."

WHAT NEEDS TO BE DONE?

- Speak with your EHR vendor to ensure it has the capability to allow you to comply.
- Review your patient access procedures - written and actual – to see if there are any impediments to access.
- Consider if any exceptions apply to certain practices that are considered important or essential.
- Update policies as necessary and update staff.
- Keep an eye on the guidance – there are still a lot of questions.

GARFUNKEL WILD, P.C.
ATTORNEYS AT LAW

QUESTIONS?

ABOUT GARFUNKEL WILD

40+
YEARS

80+
LAWYERS

4
OFFICES

- **PRACTICE AREAS:** Health Care, Litigation & Arbitration, Business, Compliance and White Collar Defense, Finance & Real Estate, HIPAA Compliance, Health Care Information and Technology, Corporate Reorganization & Bankruptcy
- **OFFICES:** New York (Great Neck and Albany), New Jersey and Connecticut
- **RECOGNITION:** *Chambers USA, The Best Lawyers in America© and Super Lawyers*

CONTACT INFORMATION

Stacey L. Gulick
t: 516.393.2264
sgulick@garfunkelwild.com

677 Broadway
Albany, NY 12207
(518) 242-7582

111 Great Neck Road
Great Neck, NY 11021
(516) 393-2200

350 Bedford Street
Stamford, CT 06901
(203) 316-0483

411 Hackensack Ave.
Hackensack, NJ 07601
(201) 883-1030