G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

LAB Compliance Advisor

For Clinical and AP Laboratories and Pathology Practices

April 2020

INSIDE THIS ISSUE

Compliance Perspectives: A 5-Step Game Plan for Protecting Lab Employees from COVID-19 Infection

In this time where so much is riding on diagnostic testing, labs face the imperative of safeguarding their employees against risks of COVID-19 infection. Here's a quick overview of the applicable laws and a strategy to comply with them, based on new OSHA guidelines.

The OSHA Duty to Prevent Workplace COVID-19 Infection

Under OSHA, employers have a duty to protect workers against workplace health and safety hazards. OSHA has made it abundantly clear that such hazards include the SARS-CoV-2 virus that causes COVID-19, even though the regulations don't mention it by name. The source of the obligation is Section 5(a)(1) of the *Occupational Safety and Health Act*, aka the "general duty clause," which requires employers to provide a workplace "free from recognized hazards" likely to cause death or serious physical harm. The duty is also implied under other OSHA standards that come into play when dealing with SARS-CoV-2, including the Personal Protective Equipment (PPE) standards (29 CFR 1910 Subpart I), which require use of gloves, eye, face and respiratory protection.

Continued on page 2

Compliance Corner: What to Do If Stark Is Keeping You from Providing Emergency COVID-19 Testing

Scenario: A local physician group wants to team up with your lab to provide COVID-19 testing for its Medicare, Medicaid and private pay patients. Although the deal would also be lucrative, the primary attraction is its potential benefits to public health and COVID-19 containment. But there's a serious compliance snag: The operating general partner of the physician group is part of the company that owns your lab. As a result, even though it would help deliver much needed COVID-19 testing to your community, you can't enter into the arrangement because you'd be violating the Stark Law.

Right?

Continued on page 11

Compliance Perspectives: A 5-Step Game Plan for Protecting Lab Employees from COVID-19 Infection, *from page 1*

The 5 Things You Must Do to Comply

While the stakes are high, COVID-19 control and response shouldn't be a challenge you're not prepared to face. If your lab already has a general plan in place to deal with and contain infectious diseases, COVID-19 response measures should be selected and carried out in accordance with that general framework. But the OSHA guidance provides useful information in applying general infectious disease response principles to the unique characteristics of and risks posed by the highly contagious SARS-CoV-2 virus. Specifically, there are five basic steps you must take to control infection hazards and ensure compliance with OSHA requirements.

Step 1: Do a COVID-19 Hazard Assessment

As with any other work hazard, the first stage in controlling COVID-19 risks is to perform a hazard assessment. The guidelines call on employers to use a four-level risk classification pyramid for assessing worker exposure risks, as summarized in Table 1.

Table 1. COVID-19 Exposure Risk Job Classifications

Risk Classification	Jobs Included in Classification
Very High	Healthcare workers, including lab personnel that collect or handle specimens from known or suspected COVID-19 patients ("COVID-19 patients")
High	• Healthcare delivery and support staff, e.g., hospital phlebotomists who must enter a COVID-19 patient's room • Medical transport workers moving COVID-19 patients in enclosed vehicles, e.g., ambulance operators
Medium	Jobs requiring frequent and/or close contact with (i.e., within 6 feet) people who may be infected with SARS-CoV-2, but aren't known or suspected COVID-19 patients, e.g., airports, retail stores
Lower	Jobs not requiring frequent and/or close contact with (i.e., within 6 feet) people who may be infected with SARS-CoV-2

Step 2: Implement Engineering Controls

The next step is to select appropriate measures to manage the COVID-19 risks of staffers based on their particular risk classification. But while the measures required will vary by classification, with very high risk jobs requiring the greatest degree of protection, the approach to selection of control measures is the same across all classifications. The first line of defense is to use engineering controls that physically eliminate or isolate the hazard. Table 2 lists examples of the engineering controls to consider for each risk classification.

LCA

Glenn S. Demby, Executive Editor

Barbara Manning Grimm, Managing Editor

Jim Pearmain, General Manager

Andrea Stowe, Business Development

Pete Stowe, Managing Partner

Mark T. Ziebarth, Publisher

Lab Compliance Advisor (ISSN 2332-1474) is published by G2 Intelligence, Plain Language Media, LLLP, 15 Shaw Street, New London, CT, 06320.
Phone: 888-729-2315
Fax: 855-649-1623
Web site: www.G2Intelligence.com.

Table 2. Engineering Controls for SARS-CoV-2 Exposure

Risk Classification	Appropriate Engineering Controls
Very High + High	*Ensure appropriate air-handling systems are installed + maintained *Placing COVID-19 patients in an airborne infection isolation room (AIIR), if there is one *Using isolation rooms, if available, to perform aerosol-generating procedures on COVID-19 patients *Using special precautions associated with Biosafety Level 3 when handling specimens from COVID-19 patients
Medium	Installing physical barriers, like clear plastic sneeze guards, if feasible
Lower	None

Step 3: Implement Administrative Controls

Administrative, aka work controls involve making the work safer by adjusting the methods used to carry it out, e.g., implementation of safe work practices.

Table 3. Engineering Controls for SARS-CoV-2 Exposure

Risk Classification	Appropriate Administrative Controls
Very High + High	• Policies that reduce exposure, like cohorting (i.e., grouping) COVID-19 patients when single rooms aren't available • Signs asking patients and family members to use disposable masks and immediately report symptoms of respiratory illness • Offer enhanced medical monitoring of workers during COVID-19 outbreaks • Provide all workers job-specific education and training on preventing COVID-19 transmission • Make psychological and behavioral support available to address employee stress • Provide emergency responders and other personnel who may be exposed while working away from fixed facilities hand rubs containing at least 60% alcohol for decontamination
Medium	• Offer face masks to ill employees and customers until they can leave the workplace • Keep customers informed about COVID-19 symptoms and ask them to minimize contact with workers, e.g., by posting signs in pharmacies where COVID-19 patients may visit • If appropriate, limit customers' and public access to the worksite, or restrict it to only certain workplace areas. • Consider strategies to minimize face-to-face contact, e.g., drive-through windows and telework • Communicate availability of medical screening or other worker health resources
Lower	*Monitor public health communications about COVID-19 recommendations and ensure that workers have access to information • Collaborate with workers to designate effective means of communicating important COVID-19 information

Continued on page 4

Compliance Perspectives: A 5-Step Game Plan for Protecting Lab Employees from COVID-19 Infection, *from page 3*

Step 4: Provide Proper PPE

The final line of defense is making sure workers have and use appropriate personal protective equipment.

Table 4. PPE for SARS-CoV-2 Exposure

Risk Classification	Appropriate PPE
Very High + High	• Gloves + gown + face shield or goggles + either: > A face mask; or > A respirator if worker works in contact with or within 6 feet of patients known to be, or suspected of being, infected with SARS-CoV-2 • Workers in labs may also need medical/surgical gowns, fluid resistant coveralls, aprons or other disposable or reusable clothing protecting additional against blood, body fluids, chemicals and other materials to which they may be exposed
Medium	Combination of gloves, a gown, a face mask, and/or a face shield or goggles depending on job and degree of exposure
Lower	None

Step 5: Provide COVID-19 Training

As it has during previous outbreaks, OSHA has stated that training workers exposed to infection risks is an essential part of COVID-19 response. By the time they complete their training, exposed workers must understand:

- What COVID-19 is;
- How the SARS-CoV-2 virus is spread;
- The risks of exposure and infection;
- How to protect themselves from those risks;
- How to recognize the signs and symptoms of COVID-19; and
- What to do if they experience such symptoms.

Managing Lab Staff: Steer Clear of 8 Pitfalls in Telecommuting Arrangements

Medical testing labs are among the "essential businesses" exempt from the mandatory workplace shutdown rules in effect across many parts of the country. Even so, telecommuting may be a desirable, if not necessary measure for at least some lab employees. And, of course, it also offers tremendous business advantages during times of normalcy. But it can also backfire if you don't make the right kind of arrangements. Here are eight telecommuting pitfalls to avoid.

1. Failing to Keep a Tight Rein on Working from Home

Pitfall: There's a dangerous tendency on the part of employees to confuse telecommuting for a license to work from home when they don't feel like coming to work. "If you're not careful, employees will begin making unilateral decisions about whether to come to work each day," warns a veteran HR director. "The moment you start getting those 'my dog is sick so I'm just going to work from home today' calls, you're in trouble," she adds.

Solution: Lay down clear and total control over when working from home is allowed. Your Policy should make it clear that what you're talking about is "telecommuting," i.e., a formal arrangement in which the employee gets permission to work from home a certain number of days or hours each week, not simply "working from home."

2. Lack of an Approval Process

Pitfall: Employees may seek to cut individual telecommuting arrangements with their supervisors. Letting supervisors approve such requests will create a tangle of separate and inconsistent telecommuting arrangements.

Solution: Establish and implement a single process for submitting and approving requests to telecommute. Best Practices: Require employees to fill out a written application form to request permission to telecommute. Designate the HR director or another individual as telework coordinator in charge of approving requests.

3. Lack of Clear Approval Criteria

Pitfall: Telecommuting is a feasible option only for certain positions and individuals. The problem is that the criteria need to be made clear. Otherwise, denying permission to telecommute could lead to grievances, discrimination suits (if the employee turned down is a minority protected by EEO law) or other legal complaint.

Example: A call center employee's application for a telecommuting position is denied based on a single incident where he was disciplined for leaving work early without permission. The arbitrator finds the employer's decision that the employee can't be trusted to work at home is unfair and arbitrary.

Solution: Establish criteria for determining who can telecommute. Criteria should be based on position. Accordingly, telecommuting won't work for technicians and testing personnel that use lab supplies and fixed equipment to carry out their jobs but may be appropriate for accounting personnel or marketers whose jobs involve extensive phone contact.

4. Lack of Clear Productivity Standards

Pitfall: Employees who work from home can't be closely monitored like other employees and are also subject to distractions, such as kids, the fridge and TV. So, it's not surprising that according to a recent CareerBuilder.com survey, only a small fraction of employees who work from home actually put in a full

Continued on page 6

Managing Lab Staff: Steer Clear of 8 Pitfalls in Telecommuting Arrangements, *from page 5*

day's work. Unfortunately, it can be tricky to fire a telecommuter for lack of productivity.

Example: Software company doesn't have just cause to fire telecommuter for lack of productivity when "there's no evidence that the employer set any standards for employees working at home."

Solution: You can minimize productivity losses by setting out clear standards for telecommuters. Best Practice: Rather than including productivity standards in your Policy, include a provision in the Policy that requires employees to sign a written telecommute contract establishing productivity standards and other specific terms of their employment while working from home, including:

- Indication of how long the telecommuting arrangement will last;
- Reservation of lab management's right to monitor telecommuters' effectiveness and periodically evaluate their performance; and
- Reservation of the right to cancel the arrangement at any time and for any reason.

5. Failure to Control Work Hours

Pitfall: Control over work hours and schedule becomes a major challenge when employees work from home. In addition to record keeping problems, it exposes you to risk of overtime claims, especially in states where employees accrue overtime for hours employers "require or permit" them to work.

Example: Computer services technician equipped with computer lines so he can remain on-call at all times gets paid overtime for hours he was "permitted to" work from home.

Solution: Set ground rules on hours worked. Require the telecommuter to reach an agreement on hours of work. Spell out the agreed-to hours in the telecommuter agreement. Set a maximum number of hours, (e.g., no more than eight hours per day) or an exact work schedule, (e.g., from 9:00 am to 5:00 pm, Monday through Friday). Another possibility is to establish a weekly maximum that employees can't exceed without first getting their supervisor's written authorization Also require telecommuters to keep and submit a weekly log of their work time so you can ensure that they're following the agreed-to schedule.

6. Failure to Provide for Telecommuter's Health and Safety

Pitfall: OSHA has issued guidance suggesting that the duty to protect workers' health and safety applies not just to the company facility or site but to any location in which workers perform their employment duties, including at home. Moreover, illnesses and injuries that telecommuters suffer in the course of their work might be deemed work-related and thus covered by workers' compensation. "Work-relatedness is determined by what employee were doing when the injury occurred rather than where they were doing it," notes one expert.

Solution: Include language in the telecommuter agreement addressing the health and safety hazards, including:

- A statement that the lab's OSHA policies and procedures, including with regard to HazCom and musculoskeletal injuries, apply to work done from home;
- A description of the physical area that makes up the work space;
- The requirement of an assessment of the hazards found in that space;
- The lab's right to access the work space to inspect or respond to hazards; and
- The employee's duty to report illnesses, injuries and safety incidents that occur at home.

7. Lack of Clear Restrictions on Personal Use of Work Equipment

Pitfall: Controlling employee misuse of lab computers, instruments and other equipment is tough enough when employees work on site. It's an even greater challenge when the employee telecommutes.

Solution: Stress in your Policy that all work equipment must be used for work purposes only. Make it clear that the telecommuter is subject to the same lab policies as site employees, including those on bullying, cyberbullying and personal use of lab equipment.

8. Lack of Clear Privacy and Information Security Rules

Pitfall: The risk of privacy and security breaches is much greater in telecommuting arrangements. Once people plug their own equipment and thumb drives into the lab's information systems, problems are bound to crop up. These problems can include computer viruses, violations of privacy laws and breaches of confidentiality.

Solution: Make sure that your policies and procedures dealing with computer usage and internet access, e.g., requirements that employees follow certain password protection and encryption procedures, apply to telecommuters. Require telecommuters to keep all files and other paperwork in a secure place. Instruct the telecommuter that these files are the lab's property and must be returned immediately when their employment ends.

Labs IN COURT

A roundup of recent cases and enforcement actions involving the diagnostics industry

SCOTUS Agrees to Step in and Resolve Obamacare Constitutionality

Case: Before COVID-19, the health care issue that kept millions of Americans up at night was the future of the *Affordable Care Act*, aka Obamacare. Having survived two constitutional challenges, the ACA is now again on trial for its life in Texas federal court. Predictably, the pace has been snail-like with the case ping-ponging between the district and appeals courts leaving patients and the insurance markets to twist in the wind. The good news is that there's light at the end of the tunnel. The US Supreme Court has agreed to intervene and hear the case on an expedited basis, rather than wait for a final ruling from the lower courts.

Significance: While no definitive schedule has been announced, experts expected the Court to hear the case sometime in the Fall of 2020, maybe even before the election. A decision would have likely come down in the spring or early summer of 2021. The problem is that those predictions didn't account for the COVID-19 situation. Still, if and when the Court does rule, Chief Justice Roberts, who twice sided with the justices upholding the law, is likely to play a pivotal role. Some legal scholars suggest that he wouldn't have taken the case if he thought the votes were there to have it declared unconstitutional. But even if that's true, there's always the chance that the Chief Justice might have miscalculated, especially if President Trump appoints what would be his third justice before the ruling comes down. The other wildcard: The Court will strike down the now legally questionable mandate requiring taxpayers to get health insurance and leave the rest of the law standing.

Taking Job at Genetic Lab Doesn't Violate Oncologist's Non-Compete with Health Data Firm

Case: Three years after becoming Senior Medical Director of Research Oncology for healthcare technology and data services company Flatiron Health, an accomplished oncologist accepted the position of Vice President of Clinical Solutions at Tempus Labs. Flatiron cried foul and sued the oncologist for violating his non-compete banning him from working for a rival company for one year after leaving the firm. But the New York federal court disagreed and tossed the claim. Although both firms provide curated data services, Tempus' principal business is its clinical lab, something Flatiron doesn't have. And because the oncologist would be working for the lab and not the data operations, the position wasn't competitive.

Significance: Courts are loath to enforce non-compete covenants, particularly in the medical field where public policy dictates that doctors and other skilled practitioners be allowed to ply their trade for the public good. Another decisive factor in this case was that the oncologist returned all Flatiron documents and devices, deleted the Flatiron email account from his phone and removed himself from company Slack groups. And the data that could potentially benefit Tempus was beyond his ken as an oncologist and way too complicated for anybody to memorize [*Flatiron Health v. Carson,* 2020 U.S. Dist. LEXIS 9782].

NantHealth Settles Fraud Suit with Shareholders for $16.5 Million

Case: NantHealth has agreed to pay $16.5 million to shareholders to settle a lawsuit accusing the company and its executives of making misstatements to artificially inflate company stock ahead of a 2016 IPO. When the truth came to light, NantHealth share prices crashed by nearly 24% in just a few hours. NantHealth hasn't admitted liability but decided that settlement made more sense than risking a trial.

Significance: Shareholders claim that NantHealth founder Patrick Soon-Shiong made statements suggesting that a $10 million philanthropic donation to the University of Utah required the University to pay the firm $10 million for genetic research services. Based on this, the company was able to puff the number of test orders it reported to investors by 50% before the IPO. Company officials also overstated the success of its GPS Cancer product, the shareholders contend.

HIPAA in a Time of Coronavirus: HHS Waives HIPAA Sanctions and Penalties

There is no doubt that we are in the midst of a national crisis, and in such times, rules have to be bent. That is happening with some parts of the privacy rules of the Health Insurance Portability and Accountability Act (HIPAA). In response to the Trump administration's declaration on March 13 that the COVID-19 outbreak is a national emergency, Secretary of the U.S. Department of Health and Human Services (HHS) **Alex M. Azar** exercised his authority to waive sanctions and penalties against covered hospitals that do not comply with some parts of the Privacy Rules of HIPAA. The waiver became effective on March 15, 2020, but is retroactive to March 1, 2020.

Background

Under HIPAA, in an emergency situation, covered entities must continue to implement reasonable safeguards to protect patient information against intentional or unintentional impermissible uses and disclosures. Further, covered entities (and their business associates) must apply the administrative, physical, and technical safeguards of HIPAA's Security Rule to electronic protected health information.

What does the Waiver Do?

Secretary Azar exercised his authority to waive sanctions and penalties against a covered hospital that does not comply with the following provisions of the HIPAA Privacy Rule:

- The requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care.

Continued on page 10

HIPAA in a Time of Coronavirus: HHS Waives HIPAA Sanctions and Penalties, *from page 9*

- The requirement to honor a request to opt out of the facility directory.
- The requirement to distribute a notice of privacy practices.
- The patient's right to request privacy restrictions.
- The patient's right to request confidential communications.

The waiver, however, is somewhat limited. The waiver only applies:

- In the emergency area identified in the public health emergency declaration.
- To hospitals that have instituted a disaster protocol, and
- For up to 72 hours from the time the hospital implements its disaster protocol.

How Long is the Waiver for?

When the Presidential or Secretarial declaration terminates, hospitals must then comply with all the requirements of HIPAA's Privacy Rule for any patient still under its care, even if 72 hours have not elapsed since implementation of its disaster protocol.

OIG Notice: OIG Warns of COVID-19 Testing Scams

Apparently, scammers aren't among the legions of people not working due to COVID-19. On March 23, the OIG issued a public service announcement and accompanying video warning consumers of scammers seeking to exploit "unsuspecting patients" by offering bogus COVID-19 tests and treatments in exchange for personal information such as Medicare numbers.

The COVID-19 Testing Scam

The scammers are deploying many of the same techniques used to perpetrate the recent genetic testing fraud targeted by the Operation Double Helix federal takedown. See *Lab Compliance Advisor* (*LCA*), Oct. 29, 2019), including telemarketing calls, social media platforms and door-to-door visits. But instead of genetic tests, they're offering unapproved and illegitimate COVID-19 testing. Just give us your Medicare number or other personal information and we'll send you the tests right away, they promise.

Of course, they use the personal information they collect to carry out bigger and more nefarious schemes, like fraudulent billing of federal health care programs and medical identity theft. And if Medicare or Medicaid denies the claim for an unapproved test, the beneficiary could be responsible for the cost.

4 Precautions

OIG is advising people to take four precautions to protect themselves from COVID-19 test scammers:

- Being suspicious of unsolicited requests for Medicare or Medicaid numbers or any other personal information;
- Being suspicious of any unexpected calls or visitors offering COVID-19 tests or supplies;
- Ignoring offers or advertisements for COVID-19 testing or treatments on social media sites; and
- Keeping in mind that a physician or other trusted healthcare provider should assess their condition and approve any requests for COVID-19 testing.

OIG is also urging consumers who believe they may have been subject to COVID-19 fraud to contact the National Center for Disaster Fraud Hotline, (866) 720-5721, or disaster@leo.gov. "We will not tolerate these scams," it declares. "With our law enforcement partners, we will be vigilant in our investigation and enforcement against those who exploit this emergency."

Compliance Corner: What to Do If Stark Is Keeping You from Providing Emergency COVID-19 Testing, From Page 1

Yes and no. Yes, the part about entering into a referral arrangement with a physician that has financial ties to your lab being a potential Stark violation is correct; however, the conclusion that you can't do the deal isn't necessarily true. **Explanation:** Because COVID-19 has been declared a public health emergency (PHE), you may be able to get a waiver allowing you to make the otherwise problematic COVID-19 testing arrangement.

When Laws Collide: Stark v. PHSA

On Jan. 31, 2020, the U.S. Department of Health and Human Services declared a PHE to deal with the COVID-19 pandemic. The action has legal consequences that providers may not be familiar with. One of them is the opportunity to secure temporary relief from Stark to provide COVID-19 testing. Here's the breakdown:

The Stark Law bans physicians from referring Medicare or Medicaid patients to labs or other health care entities with which they or an immediate family member have a financial relationship. Ensuring adherence to Stark restrictions when dealing with referring physicians is an everyday and pressing imperative for labs and their compliance managers.

The PHSA: But there's another law that may come into play, namely, the Public Health Service Act, which empowers the HHS Secretary to declare a PHE. While it may feel like public relations, the reason the Secretary made such a declaration was to activate his powers to take broad response measures to deal with COVID-19 and protect the public, which may include setting aside the normal rules of health care fraud and compliance in the interest of serving the immediate health needs of the public. More precisely, while a declared PHE is in effect, HHS may waive or modify Medicare, Medicaid, State Children's Health Insurance Program and HIPAA requirements under Section 1135 of the Social Security Act (SSA), including:

Continued on page 12

Compliance Corner: What to Do If Stark Is Keeping You from Providing Emergency COVID-19 Testing, From Page 11

- Stark Law restrictions;
- Conditions of participation;
- The need of preapproval for medical items or services; and
- Restrictions on telemedicine.

And for COVID-19, no public health need is more pressing right now than the need to deliver diagnostic testing. So, to the extent that Stark is standing in the way of that testing, it can be temporarily set aside.

Section 1135 Waivers

But Stark relief is not automatic. You must apply to CMS for and get a Section 1135 waiver before entering into COVID-19 testing arrangements with referral sources that may run afoul of Stark. and you need to get a waiver.

CMS reviews each Section 1135 waiver application on a case by case basis. If it's granted, the waiver can take effective retroactively to the start of the emergency period or to any other subsequent date CMS determines. The waiver ends upon termination of the PHE or 60 days after the waiver or modification is first published. If the PHE is still in effect after 60 days, it can be renewed for additional 60-day periods.

Takeaway

During the current COVID-19 emergency, labs need to recognize that they may have additional latitude to enter into temporary arrangements with physicians to promote public health. More precisely, seeking a Section 1135 waiver may make a lot of sense if your lab has an opportunity to provide coronavirus testing or other related services for Medicare or Medicaid beneficiaries in collaboration with a physician or medical group that has ownership interests in or other financial ties to your lab that would normally be prohibited under the Stark Law.

G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA
LAB Compliance Advisor
For Clinical and AP Laboratories and Pathology Practices

Important Notice: G2 Intelligence Moves to Digital-Only Publishing Format

As you know, American business is being hit hard by the COVID-19 pandemic.

The impact upon the publishing and media industry, and our critical suppliers and vendors, is growing increasingly severe. We are uncertain of our ability to continue to produce and deliver print versions of our publications, and we see no clear timeframe for resolution.

Therefore, G2 Intelligence has made a decision to move to a Digital-Only publishing format for the immediate future. All G2 newsletters, reports, and other information services will continue to be available in digital format to help support the lab industry during this crisis, but print versions will be discontinued.

Accessing your G2 products digitally (email, pdf, website, and other electronic formats) has many advantages, including more rapid distribution of important content, access to archives, and a content-rich website that offers many additional special features and benefits for our Members.

Additional improvements will be phased in over the coming months.

Fortunately, most of our Members already receive their G2 publications digitally. If you are already a digital Member, there will be no visible impact upon your service. But if you receive your publications print only, we need your email address to convert you to digital distribution. If you receive multiple copies, we need the email addresses of all those in your organization who are members so they continue to receive their product. A G2 representative will be in touch with all our print only Members to help you make an easy transition and answer any questions.

If you have any questions,or you wish to update your email information, please contact **Andrea** at **888-729-2315, ext 316**.