

March 2018

## INSIDE THIS ISSUE

### SCORECARD

Recent Urine Testing  
False Billing Cases ..... 3

### LABS IN COURT

A roundup of recent cases and enforcement actions involving the diagnostics industry ..... 5

### TRAPS TO AVOID

Aetna, HIPAA and the \$17+ Million Envelope Mishap ..... 6

### TOOL

Model Pandemic Influenza Policy ..... 7

6 Pandemic Preparation Privacy Pointers ..... 10

Pandemic, Privacy & Practical Limits ..... 12

[www.G2Intelligence.com](http://www.G2Intelligence.com)



## Upcoming Events

### Lab Leadership Summit

*Designing, Implementing & Managing a High-Profit Lab Outreach Program*

Friday, April 27, 2018

[www.lableadershipsommit.com](http://www.lableadershipsommit.com)

### Lab Institute 2018

Oct. 24-26, Washington, DC

[www.labinstitute.com](http://www.labinstitute.com)

## Enforcement Trends: Opioid Crackdown Zeroes in on Urine Drug Testing—Today the Doctors, Tomorrow the Labs

**A** 67-year-old Michigan M.D. is the most recent doctor taken down in what has become a crucial part of the federal government’s opioid drug crusade: urine tests ordered by prescribing physicians to be performed at the labs they own. On Feb. 6, Dr. Rodney Moret pleaded guilty to using his pain management and HIV infusion clinic as a “pill mill.” In addition to illegally dispensing \$15 million worth of prescription drugs, including controlled substances Hydrocodone, Alprazolam, and promethazine with codeine cough syrup, the doctor billed Medicare for \$6 million worth of tests that were either not medically necessary or not performed at all. Sexually molesting and harassing female patients made an ugly situation that much more hideous and surely weighed in the judge’s decision to sentence the doctor to 75 months’ imprisonment.

*Continued on page 2*

## Compliance Perspectives: Avoid Privacy Pitfalls in Pandemic Planning & Response

**A**lthough not officially a pandemic, the 2018 flu season has been the worst in nearly a decade. So why not use it as an opportunity to review your lab’s pandemic preparations—or, if you haven’t already done so, start the preparation process? In so doing, you need to account for something that tends to go overlooked in pandemic planning: the privacy ramifications. After all, many if not some of your pandemic measures will require you to collect, use and disclose personal information about your employees. For example, you might have to ask employees if they have a medical condition that increases their vulnerability to flu. This article explains pandemic preparation privacy risks and how to avoid them.

### The Privacy Rights of Your Employees

Most employees do have some privacy rights vis-à-vis their employers. But the scope and extent of those rights differ depending on how and where your lab operates and the type of personal employee information involved. Thus, while HIPAA is

*Continued on page 9*

## G2CA

Glenn S. Demby,  
Editor

Lori Solomon,  
Contributing Editor

Catherine Jones,  
Contributing Editor and  
Social Media Manager

Barbara Manning Grimm,  
Managing Editor

David van der Gulik,  
Designer

Randy Cochran,  
Corporate Licensing Manager

Myra Langsam,  
Business Development

Michael Sherman,  
Director of Marketing

Jim Pearmain,  
General Manager

Pete Stowe,  
Managing Partner

Mark T. Ziebarth,  
Publisher

Notice: It is a violation of federal copyright law to reproduce all or part of this publication or its contents by any means. The Copyright Act imposes liability of up to \$150,000 per issue for such infringement. Information concerning illicit duplication will be gratefully received. To ensure compliance with all copyright regulations or to acquire a license for multi-subscriber distribution within a company or for permission to republish, please contact G2 Intelligence's corporate licensing department at myra@plainlanguage.com or by phone at 888-729-2315. Reporting on commercial products herein is to inform readers only and does not constitute an endorsement.

**G2 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](http://www.G2Intelligence.com).

### ■ Enforcement Trends: Opioid Crackdown Zeroes in on Urine Drug Testing, from page 1

This is big news. And while CLIA review and reform will take months (if not years) to complete, lab compliance officers should waste no time in bringing it to the attention of their CEO and executive team. Here are the key points to cover in your briefing.

### The Urine Testing Gold Mine

Best known for its employment applications, urine testing is also medical protocol for patients prescribed opioid drugs. Urine tests are used to ensure patients are not developing addictions and confirm they are actually taking the meds rather than selling them on the black market. Not surprisingly, then, increases in opioid prescriptions have coincided with increases in utilization.

The price of tests has also gone up as many labs scrapped the simple test cup and testing strip methods in favor of high tech testing machines. These installed machines offered another financial advantage: Under Medicare rules, each individual drug tested for could be billed individually.

All of this has caused urine testing reimbursements to skyrocket. Thus from 2011 to 2014, Medicare and private insurer spending on urine screens and related genetic tests quadrupled to roughly \$8.5 billion per year, according to Kaiser Health News and Mayo Clinic analysis. In 2014, the federal government paid more in urine drug tests than for the four most recommended cancer screenings *combined*.

Among the biggest beneficiaries of this spending are physicians that operate their own testing labs typically as part of a pain management clinic a la the Michigan example above. Bloomberg reports that in 2014-2015, Medicare paid over 50 different pain management practices at least \$1 million for drug-related urine tests. According to Bloomberg, 31 pain practitioners derived at least 80% of their Medicare income from urine testing.

### The Feds Smell a Rat

Of course, none of this has been lost on the feds. Back in 2010, CMS tightened up on billing for simple urine screens. But the new rules did not cover machine testing. Prosecutors, too, began taking note of the spike in reimbursements and the incongruously high rates for what were thought to be simple tests. The remark of a Jacksonville, Florida assistant U.S. attorney reportedly quoted in Bloomberg sums up the attitude: "We're focused on the fact that many physicians are making more money on testing than treating patients. It is troubling to see providers test everyone for every class of drugs every time they come in."

### The Millennium Case

The enforcement breakthrough came in 2011 when one of the country's leading billers of urine drug tests, Millennium Health LLC, faced an onslaught of whistleblower suits for allegedly billing Medicare and Medicaid for millions in unnecessary urine drug and genetic tests and providing freebies to physicians in exchange for referrals. The Justice Department picked up the case

and in October 2015, Millennium agreed to fork over \$256 million to settle the claims. Faced with such a liability, Millennium soon filed for bankruptcy.

### The Opioid Epidemic Effect

The seeds for a crackdown on urine sowed earlier have been brought into full bloom by the opioid epidemic. The issue has morphed from financial rip-off to full blown national health crisis. What is being questioned now is not simply the billing or even ordering of the tests but the underlying decision to prescribe opioids in the first place. Accordingly, during the recent explosion of opioid abuse cases, physicians and not labs have been the primary target. (See the box below for an overview summary of the key cases.)

*Takeaway: Impact on Your Labs. While testing labs are not the prime concern, they are still an integral part of the case. In the early cases labs have come into play only to the extent they were part of the ordering physician's "pill mill" operation. Accordingly, labs owned or operated by physicians currently have the most to fear. But that is bound to change. The opioid crackdown is just starting and it is only a matter of time before hospital and independent labs come under scrutiny. Bottom Line: Any and every lab that is involved in urine drug testing of opioid patients, whether physician-owned or independent, has to be on high alert.* 

## SCORECARD: Recent Urine Testing False Billing Cases

Increasing utilization rates and higher prices have made urine drug testing related to prescription opioids a red flag for CMS, the Justice Department and whistleblowers for a number of years. And now the opioid epidemic has not only intensified the scrutiny but turned it into a national health emergency of the first order. The result has been a spate of federal and state cases targeting urine testing abuses that kicked off this summer and is likely to continue for years to come. Here is a chronological summary of the leading cases that have come down so far.

### August 2018—Louisiana

The co-owner and billing manager of a spine and pain management clinic were charged with falsely billing Medicare and private insurers for \$4.4 million worth of medically unnecessary services, including \$3.9 million in quantitative urinalysis tests. The clinic was planning to open a urinary testing lab and began storing specimens for unnecessary testing once the lab went on line, the indictment claims.

### September 2018—Tennessee

Federal prosecutors charged urine testing lab Confirmatrix Labs with paying kickbacks to "pill mill" operators that dispensed medically unnecessary opiates for referring patients to the lab for urine testing the patients had to undergo to take the meds. Confirmatrix then allegedly billed the state Medicaid program TennCare for the whole shebang via a series of Confirmatrix shell companies. Neither Confirmatrix nor its officials have been charged. However, they may be on borrowed time. The lab's founder has a track record and served three years in federal prison for running a massive music counterfeiting operation. Another red flag is Confirmatrix's abnormally high per-patient costs. One private study named the lab "the biggest outlier" among reviewed firms for Part B payments.

### October 2018—Michigan

A 72-year-old physician pled guilty to conspiring with two other Detroit-area providers, including the owner of the Tri-County Network, in carrying out an opioid drug scheme that generated roughly \$19 million in fraudulent Medicare billings. *The doctor's role:* prescribing medically unnecessary oxycodone, opana and hydrocodone to Medicare patients, many of whom were drug addicts; directing physicians to make Medicare patients that wanted an opioid prescription to first undergo medically unnecessary facet joint injections and lab tests; and telling physicians to refer those services to labs, clinics and other facilities in which he had secret ownership interests.

### November 2018—Florida + Maryland

This particularly smarmy scheme involved a South Florida network that offered free rent and other kickbacks to physicians in exchange for referrals of insured drug addicts to reside in their sober homes. Residents were then subjected to regular drug testing. The network medical director created a drug testing regimen for each resident, including many he never actually examined, based on the bribes he got from the testing lab. He then used higher paying codes to bill Medicare for the exams. Adding insult to injury, residents were allowed to continue doping as long as they kept their mouths shut. Among the four defendants, the medical director was sentenced to 48 months in prison and one year of supervised release and a doctor had to pay \$2.198 million to make restitution for the money he stole.

Two doctors at a Maryland pain management clinic took bribes kickbacks to prescribed pain relief medications and refer urine tests to a New Jersey lab. Six defendants were charged: four pleaded guilty; one, a doctor, committed suicide, and the other, also a doctor, went to trial and was convicted of 26 felony charges and now faces up to 99 years in prison.

### December 2018—Connecticut

A substance abuse clinic and its CEO settled claims of incorporating on-site testing of patients into the bundled weekly rate it charged the Connecticut Medicaid Program for all services rendered. The problem is that it was referring those tests to an independent lab in Massachusetts, meaning Medicaid was paying twice for those tests. *The settlement bill:* \$883,859.

### January 2019—Indiana

A husband-and-wife physician team were charged with falsely billing Medicaid for over \$1.1 million in urine drug tests. The government contends that from 2011 to 2013, the now retired physicians routinely required patients seeking opioid prescriptions to furnish a urine specimen to be tested for nine different classes of drugs using a multiplex screening kit costing no more than \$5 per day. They then billed and were paid \$171.22 per patient, getting around the \$20.83 per patient limit allowed under Indiana Medicaid billing rules by falsely certifying that they had collected and tested nine separate samples.

### February 2019—Indiana

A 67-year-old Michigan M.D. pled guilty to using his pain management and HIV infusion clinic as a "pill mill." In addition to illegally dispensing \$15 million worth of prescription drugs, including controlled substances Hydrocodone, Alprazolam, and promethazine with codeine cough syrup, the doctor billed Medicare for \$6 million worth of tests that were either not medically necessary or not performed at all. Sexually molesting and harassing female patients made an ugly situation that much more hideous and surely weighed in the judge's decision to sentence the doctor to 75 months' imprisonment. 

# Labs IN COURT

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

## ACLA Goes for Jugular in PAMA Challenge Case

**Case:** Attorneys for the American Clinical Laboratory Association asked the federal court for summary judgment in its lawsuit challenging the legality of the new PAMA-based Medicare Part B fee schedule for lab tests. Specifically, ACLA contends that the HHS exceeded its authority and ignored the PAMA legislation by omitting hospital and reference labs from pricing data used to set fee rates for lab services under the law. (For more about the lawsuit, see [GCA, Dec. 11, 2017](#).)

**Significance:** If the court does grant summary judgment it would essentially be saying that it has enough basis to rule that ACLA's claims are legally valid without holding a trial. If it denies the motion, a trial will be necessary—unless, that is, HHS brings and wins its own summary judgment motion.

## Individual Officers Called to Account for Role in HDL Scam

**Case:** Three years after Health Diagnostics Laboratory, Inc. (HDL) and its marketing partner BlueWave Healthcare Consultants—both now defunct—settled federal kickbacks claims for \$50 million, the individuals involved in the scheme have been brought to justice. On Jan. 31, a federal jury in South Carolina unanimously convicted HDL's former CEO and BlueWave's co-owners of conspiring to pay doctors sham specimen processing and handling fees of \$17 and routinely waiving copays and deductibles in exchange for referring Medicare and Tricare to HDL and its partner Singulex for medically unnecessary blood testing. But the \$16 million damage award the jury returned was far below the \$174 million the DOJ asked for.

**Significance:** For sheer dimensions, the HDL scheme has been described as among, if not the biggest case of lab fraud ever. In many ways, it also represents the new dynamic of federal healthcare fraud enforcement, not simply because it began as a whistleblower suit (actually, a series of three suits) but in its following of Yates Memo principles of separating the corporation from its individual principals and going after each group separately. This strategy represents a dramatic departure from previous DOJ policy of focusing on the corporate entity and allowing the individuals to avail themselves of the corporate liability shield and legal defense.

## llumina Wins \$26.7 Million in Patent Infringement Damages

**Case:** Illumina won a patent infringement lawsuit against Ariosa Diagnostics in the US District Court of the Northern District of California. The case began in 2014 when Illumina claimed that Ariosa's test for "simultaneous quantification of hundreds of DNA loci" infringed the former's patent covering methods for amplifying and genotyping samples simultaneously. That same year, Roche acquired Ariosa and created a microarray version of the test. So Illumina filed a second suit claiming that the new test also infringed. The jury agreed with both claims and awarded Illumina \$26.7 million in damages.

**Significance:** The case may not be over. General counsel for Roche Molecular Solutions is quoted as saying in an email that the company is disappointed" with the decision and is reviewing its legal options. Stay tuned.

## Fresenius Settles HIPAA ePHI Charges for \$3.5 Million

**Case:** HIPAA requires providers to perform a thorough risk assessment of the systems they use to secure electronic personal health information (ePHI) and correct the vulnerabilities they identify. On Feb. 1, the federal agency that enforces the HIPAA rules, the HHS Office for Civil Rights, announced that Fresenius Medical Care North America has agreed to fork over \$3.5 million to settle charges of failing to meet this obligation at five of its facilities. The specific forms of violation varied from facility to facility—lack of procedures for incident response, no policies for removing hardware and electronic media containing ePHI within and outside the facility, inadequate encryption, failure to prevent unauthorized access, etc.

**Significance:** Although the \$3.5 million fine stings, the real pain point for Fresenius may be the onerous corrective action plan that OCR imposed on the affected facilities, including the obligation to:

- ▶ Conduct a top-to-bottom HIPAA compliance audits;
- ▶ Submit a Risk Management Plan based on the audit findings to HHS for approval;
- ▶ Submit separate written reports on encryption measures and device and media controls;
- ▶ Develop and implement an enhanced privacy and security awareness training program; and
- ▶ Deliver annual reports and training reports. 

## Traps to Avoid: Aetna, HIPAA and the \$17+ Million Envelope Mishap

**W**hen mailing sensitive personal medical information to patients, it is probably best to avoid transparent window envelopes. One of America's biggest health insurance companies just learned this lesson the hard way—to the tune of \$17.2 million.

### The Lawsuit

That staggering total is what Aetna agreed to pay on Jan. 16 to settle a federal class action lawsuit by beneficiaries accusing the insurance giant of compromising their privacy by mailing them HIV medication information in an envelope with a transparent window. The July 2017 mailing which inadvertently revealed the patient's name, address and start of the letter, was sent to 12,000 beneficiaries taking medication for HIV, or PrEP, a pre-exposure prophylactic pill to prevent HIV. Ironically, Aetna sent the letter in response to beneficiaries' privacy concerns about having to obtain their HIV meds from mail-order pharmacies.

### The Fallout

The story takes on a grotesque dimension when you consider the hundreds of millions of dollars firms like Aetna invest each year to secure the personal medical data with which they are entrusted from high-tech hacking and cyber-attack. But to the extent it serves as a reminder of the potential of low-tech breaches to do life-shattering privacy damage, the Aetna debacle might prove a long-term positive.

### The Takeaway

First and most obvious, remember that window envelopes and medical information can be hazardous mix. As for post cards, don't even think about it. Finally, labs and other providers would do well to take heed of the privacy measures the settlement agreement imposes on the administrator in charge of executing and notifying the affected Aetna beneficiaries of the settlement:

- ▶ The envelope containing the notice must obscure the envelope's contents;
- ▶ The return address must be devoid of any identifying information other than a P.O. box, city, state and ZIP Code; and
- ▶ There must be a statement on the envelope front stating: "Confidential Legal Information—To Be Opened Only By The Addressee." 

## TOOL: MODEL PANDEMIC INFLUENZA POLICY

Although not officially a pandemic, the miserable 2018 flu season is a vivid reminder of the importance of preparing so that your lab responds effectively if and when the next pandemic does hit. The starting point is a pandemic policy like the one below. Drawing on actual examples used by government agencies and private companies, the Model Policy can be adapted for use by your own lab.

### XYZ LABORATORIES PANDEMIC INFLUENZA POLICY

#### 1. PURPOSE

This Policy, which is Part of XYZ Laboratory's ("LAB") emergency-preparedness and business continuity plan, is designed to set broad parameters for safeguarding employees' health and well-being during a flu pandemic while ensuring our ability to maintain essential operations and continue providing essential services to our customers.

#### 2. DEFINITION OF PANDEMIC INFLUENZA

According to the federal Centers for Disease Control, the Occupational Safety and Health Administration and other organizations, influenza or flu is caused by a variety of influenza A viruses that can cause at least three different diseases:

1. Avian flu viruses that mostly affect birds and chickens or other poultry;
2. Pandemic influenza that can occur when mutating flu viruses become transmissible to humans, who generally lack any natural immunity to fight off the viruses' adverse health effects; and
3. Seasonal flu.

Of the three, pandemic influenza poses the most serious global threats to public health, the economy and LAB operations.

#### 3. ESSENTIAL PERSONNEL

LAB expects that during a pandemic, only the employees it has identified and designated as essential personnel will be available for work. LAB acknowledges, however, that even essential personnel might become ill and unavailable to work or not be able to reach our worksite because of conditions beyond their own or LAB's control. Consequently, LAB and its industry partners will make back-up arrangements so that designated personnel in locations outside our respective areas are trained and equipped to fulfill the duties of unavailable essential employees. LAB has also equipped essential personnel with all resources necessary to work remotely during emergencies.

#### 4. REMOTE WORK LOCATIONS

During an influenza pandemic, local, state, or federal authorities might prohibit or severely curtail access to and use of public services and public transportation; close or prevent access to buildings or public highways; isolate or quarantine buildings' occupants; and prevent inter- or intrastate delivery of goods and services. LAB cannot predict and has no control over such actions and acknowledges its legal duty to comply with outside authorities' directives. It is, however, prepared to continue key "bare bones" operations from remote work locations, including essential employees' home offices. LAB has installed at all remote work locations all the equipment necessary for off-site telecommuting operations and designated a secure web site through which essential personnel can communicate with each other and outside authorities.

#### 5. INFECTION CONTROL

LAB takes steps to minimize exposure to and spread of infection in the workplace and recommends measures that employees can take to protect themselves outside the workplace and encourages all workers to discuss their specific needs with a family physician or other appropriate health or wellness professional.

#### 6. EMPLOYEE OBLIGATIONS

LAB expects employees who contract the flu or have been exposed to infected family members or others to stay home and seek medical attention as necessary and appropriate. It expects such workers to notify LAB as soon as possible of exposure or illness. At LAB's discretion or the direction of outside authorities, it can require the isolation and quarantine of any infected employees who come to work despite exposure or need for medical attention.

#### 7. VACCINATION

LAB requires all essential personnel to maintain up-to-date vaccinations and to obtain annual LAB-paid flu shots, if available and not medically contraindicated. LAB requires essential personnel to certify that they have

obtained the necessary inoculations and to maintain a copy of that certification, which must be provided at LAB's request.

## 8. EMPLOYEE TRAINING

All employees are at risk of exposure to flu viruses, both in and outside the workplace; therefore, LAB requires all employees to attend initial or refresher training annually in September to become informed about what to do when a flu outbreak occurs covering such issues as availability of flu shots, symptoms and health effects of influenza, treatment, and sources to contact for appropriate medical care, steps to take if exposure is suspected; LAB representatives to whom to report known or suspected exposures, and procedures for reporting exposure to co-workers, family members, friends, or others who are ill with flu; proper use of LAB-provided personal-protection equipment; proper hygiene in the workplace and at home; and communications. Training includes role-plays based on scenarios developed to test employees' understanding of our planned emergency response. Supervisors are responsible for recording and maintaining documentation on every employee's participation in required training.

## 9. PERSONAL PROTECTIVE EQUIPMENT

LAB maintains on site adequate supplies of recommended personal-protection equipment, such as face masks, eye protection, rubber gloves, and anti-bacterial hand gels and wipes, which workers may be required to use. All employees are advised to speak with their personal physician about types and proper use of personal-protection equipment in the home.

## 10. FACILITIES MAINTENANCE

LAB's facility manager regularly inspects the workplace for signs of heating, air conditioning, or other equipment in need of replacement or repair and coordinates closely with our cleaning and waste-removal contractors to maintain our physical plant in top condition. LAB approves the installation or use wherever possible of improved equipment or cleaning methods to guard against the spread of infection in the workplace.

## 11. EMPLOYEE LEAVE AND PAY

In the event of pandemic influenza, LAB grants all non-essential personnel immediate administrative leave. It pays workers on administrative leave a reduced salary, and continues such reduced salary for one-week periods up to a maximum of six weeks. LAB monitors emergency conditions daily to determine how long administrative

leave must continue and, following consultation with outside authorities, advises employees when to expect to return to work.

LAB places on family and medical leave any workers who fall ill with flu or must be absent from work to care for an infected family member. Such employees must notify LAB as soon as possible of need for family and medical leave. Employees may use accrued paid annual and sick leave in lieu of unpaid family and medical leave. Employees must take unpaid family and medical leave once all accrued paid leave is used. All employees are also required to certify that they have received, read, and fully understand our family and medical leave policy and its use in a flu outbreak.

## 12. BUSINESS TRAVEL

All reasonable efforts will be made to eliminate the need for travel by taking advantage of technology. Generally, in the event of an influenza pandemic, travel on LAB's behalf will be immediately suspended and limited to a select group of essential personnel who have obtained required travel authorizations from LAB and any necessary outside authorities. Essential personnel or other employees traveling anywhere on LAB's behalf and exposed to avian flu or pandemic influenza are eligible for workers' compensation.

## 13. EMERGENCY CONTACT INFORMATION

Employees must notify their immediate supervisor and HR of any change in emergency contact information within two weeks of a change. When providing such information, employees, especially those who have children or care for elderly relatives, should identify individuals on whom they can depend if the employees themselves become sick at work and must be isolated and quarantined. HR is directed to verify electronically employees' emergency contact information twice a year, in January and July. Supervisors are required to maintain in the workplace and at home an up-to-date emergency-contact list for their unit or department.

## 14. SPECIAL NEEDS AND ACCOMMODATIONS

LAB is required by law to notify first-responders about employees with medical conditions that could be compromised because of an influenza pandemic. Such employees are urged to confidentially self-identify to HR so that we are aware of and can prepare for you to receive any special medical expertise you might require if you become severely ill on the job. HR maintains the confidentiality of any information you provide, making it available solely on a need-to-know basis and only when needed by emergency responders.

### ■ Compliance Perspectives: Can You Require Lab Workers to Get a Flu Shot, From Page 1

about patient rather than workplace privacy, it comes into play when labs and other employers seek to collect, use and disclose (for simplicity's sake, we'll refer to all three of these verbs collectively as "use," unless the context requires otherwise) personal health information about their employees. Workplace-related privacy rights of employees may also stem from:

- ▶ State personal privacy laws, both statutory and common law, i.e., law made by courts in individual cases that form precedent for subsequent cases;
- ▶ Provisions of employment contracts, both individual non-union and especially collective bargaining agreements affecting union employees;
- ▶ Privacy assurances contained in your own HR policies and Codes of Conduct; and
- ▶ Any other things you do to foster reasonable expectations of privacy of your employees.

### The Practical Impact of Employee Privacy Rights

The most significant privacy restriction for labs, especially in the flu and infectious disease control context, is the requirement to get employees' consent to use their medical and other personal health information. Getting proper consent is an issue unto itself. The consent form must be clearly written so the employee knows what she's signing; and the decision to sign the form must be totally voluntary. Any signs of trickery or coercion nullify the consent.

However, as a practical restriction, consent is sometimes overrated. *Explanation:* Where privacy restrictions do exist, they are subject to exceptions allowing for use of personal information for a wide variety of purposes *without* consent. As explained by a leading privacy attorney (who, fittingly perhaps, asked not to be quoted by name), "an employer has a legitimate need to collect, use and disclose certain types of personal information about employees in order to operate the business and fulfill its obligations to employees." Examples of legitimate functions for which consent-less use of an employee's health or other personal information is generally justified:

- ▶ Verifying the employee's eligibility for sick leave or disability benefits;
- ▶ Determining what accommodations to make for employees or job applicants with physical or mental disabilities required by the ADA; and
- ▶ Filing workers' compensation claims.

### Rule 1: Consent MAY BE Required for Pandemic Planning

If you take just one thing from this article, let it be this: It is unclear whether pandemic preparation and response is a function that falls into the use-without-consent category. Equally unclear, then, is whether employees are required to provide you the personal health information your lab needs to make preparations for pandemic. *Bottom Line:* You may need and should probably acquire employees' consent to use their personal employee information for pandemic planning.

### Rule 2: You Must Keep Personal Information Used to Minimum Necessary

Use of personal information must also be kept to the minimum necessary to accomplish whatever pandemic planning or response function you need the information to carry out. Thus, for example, it would be inappropriate to ask employees to undergo a physical exam or submit a complete medical record to assess their vulnerability to infection. Note that the minimum necessary restriction applies regardless of whether the use is consented to.

### Rule 3: You Must Notify Employees of Information Use

You also need to notify employees of the personal information you use and why you need it for pandemic planning and response. “Transparency is an essential principle of personal privacy rights,” our attorney expert explains.

### Rule 4: Information Must Be Kept Secure

Labs and other employers must maintain the security of any personal health information they collect from employees. Security measures include:

- ▶ Physical barriers such as keeping files locked;
- ▶ Electronic measures such as password protection and encryption; and
- ▶ Administrative controls such as keeping the number of staffers with access to the information limited to the minimum necessary.

### Rule 5: Information Must Be Properly Destroyed After Use

Finally, you must ensure that the personal information you collect from employees for pandemic planning and response is properly destroyed after it's no longer needed.

## 6 PANDEMIC PREPARATION PRIVACY POINTERS

Here are some of the specific things you can and can't do to ensure that your pandemic planning and response activities don't violate employees' privacy based on government guidelines, expert opinions and privacy best practices:

### 1. Identifying Employees Who May Need Alternative Work Arrangements

**Situation:** You generally have no right to ask employees who they live with. But gathering this information could become important to pandemic planning to the extent it enables you to determine which employees might have to make alternative work arrangements.

**Wrong:** Asking: “Do you have young children or elderly parents at home that you might have to stay home and care for in the event of a flu pandemic?”

**Right:** Distribute a survey asking employees if they may have to make alternative work arrangements to care for kids or elderly parents. This way, you will be able to estimate how many employees may be absent without collecting detailed personal information.

### 2. Identifying Employees Who Might Be Susceptible to Infection

**Situation:** You might want to warn any employees that have asthma, immunity deficiencies or other medical conditions that make them vulnerable to the flu to get vaccinated and take special precautions. But asking about an

employee's general medical condition may also be a privacy violation.

**Wrong:** Asking employees to furnish detailed information about their medical condition, e.g., making them tell you if they have asthma.

**Right:** Let all employees know that individuals with certain kinds of conditions are at risk and need to consider taking additional precautions.

### 3. Asking Employees If They've Been Vaccinated

**Situation:** You have an obvious interest in knowing if your employees have been vaccinated. But this again is personal information.

**Wrong:** Asking employees: "Have you and your family members gotten your flu vaccine?"

**Right:** Encouraging employees to get vaccinated and giving them information about vaccinations, such as vaccination clinic schedules.

### 4. Asking Employees for Personal Contact Information

**Situation:** Assuming you don't already have this information, you may want to ask employees for contact information they can use to provide updates about a pandemic situation. But this is private information that employees might be loath to provide.

**Wrong:** Asking—and especially requiring—employees to give you their personal email or phone number.

**Right:** Asking employees to advise you how they prefer to be contacted and giving them alternative ways to get information from you without having to disclose their private contact information, such as having the employee agree to call in to the office at agreed-upon intervals.

### 5. Asking Employees Who Call In Sick If They Have the Flu

**Situation:** In a pandemic, you'll probably want to keep track of how many employees are diagnosed with the flu.

**Wrong:** Asking employees who call in sick: "What's wrong with you? Do you have the flu?"

**Right:** Asking employees who say they're sick how long they expect to be out and when they plan to return. In short, asking for a prognosis is okay; but asking for a diagnosis is not.

### 6. Notifying Other Employees that a Co-Worker Has the Flu

**Situation:** If managers learn that an employee has the flu, they might want to notify others at the lab, including the employee's co-workers.

**Wrong:** Disclosing an employee's diagnosis to somebody else within the lab is just as impermissible as asking an employee to furnish his diagnosis to begin with.

**Right:** Letting others know that the employee isn't available, and if necessary, when he's expected to return.

### Pandemic, Privacy & Practical Limits

⊗ What You CAN'T Do	☑ What You CAN Do
Ask: "Do you have kids or older parents that you might have to stay home and care for?"	Hand out a survey asking employees if they might have to make alternative work arrangements without specifically asking who they live with.
Ask: "Do you have asthma or other medical condition that makes you at high risk of infection?"	Notify ALL employees that certain medical conditions heighten the risk of infection and advise any employee who has such conditions to take special measures to protect themselves.
Ask: "Have you and your family been vaccinated?"	Encourage employees to get vaccinated and provide information, such as vaccination schedules and clinic locations, to help them do so.
Asking employees for personal emails or other contact information in case you need to notify them of pandemic developments.	Ask employees what contact arrangements they want to make and explore ways to maintain contact that don't involve getting private emails, e.g., letting employees call in themselves at agreed intervals.
Asking an employee who calls in sick: "Do you have the flu?"	Asking an employee who calls in sick: "How long do you expect to be out of work?"
Telling an employee's colleagues: "Joe has the flu."	Telling an employee's colleagues: "Joe has called in sick and isn't expected to return until Thursday."



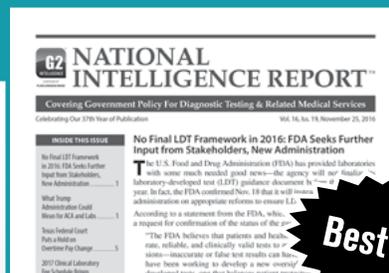
## Special Offer for G2 Compliance Advisor Readers

Test Drive G2 Intelligence Memberships for Just \$47 for 3 Months



#### Lab Industry Report

The place the lab industry turns for business intelligence and exclusive insight into what's happening to key companies, as well as the Wall Street view on the lab industry, the latest analysis of mergers, buyouts, consolidations and alliances.



#### National Intelligence Report

From Stark and Anti-Kickback to Medicare and congressional lobbying efforts, NIR keeps you updated and richly informs your business planning and risk assessment.



#### Diagnostic Testing & Emerging Technologies

News, insider analysis, statistics and forecasts on the important innovations, new products, manufacturer's, markets and end-user applications vital to the growth of your lab.

**Best Deal!**

Contact Myra at 888-729-2315 or Myra@PlainLanguageMedia.com for details on this special offer.

To subscribe or renew G2 Compliance Advisor, call 888-729-2315

Online: www.G2Intelligence.com Email: customerservice@plainlanguagemedia.com

Mail to: Plain Language Media, PO Box 509, New London, CT, 06320 Fax: 855-649-1623

Multi-User/Multi-Location Pricing? Please contact Myra Langsam by email at: Myra@PlainLanguageMedia.com or by phone at 888-729-2315.