

Evidence Collection

The Whistleblower Guide

◆ Take what you need; don't take everything.

You do not need *everything*. Collect material that supports your claim, including evidence that the government paid a fraudulent claim. Avoid downloading massive files or entire hard drives. The information you gather should be specific and significant.

DO...*gather as much information as you can and collect information related to claim.*

DON'T...*download indiscriminately or collect unrelated documents/files.*

◆ Only look where you have access; don't snoop.

Collect information and files that YOU have access to. Do not attempt to gather or retrieve records that you are not authorized to access (or view). Never try to access materials after being terminated or suspended. Make sure to preserve evidence showing that you had legitimate access to any information you gathered.

DO...*collect records you have legitimate access to.*

DON'T...*use someone else's credentials or attempt access post-termination.*

◆ Be careful; don't set off alarms.

Unusual activity could raise suspicion and red flags. Try to maintain your usual activity patterns, and avoid saving or sending information from devices owned by your employer. Be mindful of your employer's device and network monitoring capabilities. Use your personal devices to capture images whenever possible. If you cannot access evidence without raising suspicions, keep notes of where the information is located and what it looks like.

DO...*collect information lawfully and be discreet.*

DON'T...*use company email, file, or cloud services to save information or send it to yourself or your attorney.*

◆ Keep even potentially privileged records separate.

All communication with your company's attorneys is privileged and may not be used in the investigation. However, not every member of the legal team is an attorney, and not every attorney works for the legal team. Review all parties on emails and in meetings before you pass them along to your lawyer to avoid "tainting" your claim. If you are not sure, err on the side of caution and do not provide the information.

DO...*carefully review confidential information from all sources and parties involved .*

DON'T...*collect information information from the company attorneys.*

◆ Talk to your lawyer; don't talk to anyone else.

Discussion of the whistleblower process with anyone who is not your attorney may jeopardize your claim. Be careful when speaking with coworkers or potential witnesses, as they may decide to file their own claim, report you to the company, or otherwise endanger your case. If you have questions, your attorney is there to help!

DO...*ask your attorney questions and share your concerns.*

DON'T...*share information with anyone else.*

Evidence Collection

The Whistleblower Guide

Document Checklist

Internal Communications & Audit Evidence

Documents showing knowledge, intent, or concealment

- Emails demonstrating operational knowledge of fraud
- Audit findings
- Timesheets
- Payroll records

Contracts, Policies, & Operational Documents

Materials showing obligations, performance, and internal rules

- Master Service Agreements
- Performance reports
- Standard Operating Procedures to “fix/alter” billing
- Training records

Billing, Claims, & Financial Documents

Materials tied to what was billed, how it was coded, and what the government paid

- Claims forms
- Proof the government paid for the alleged fraudulent goods/services
- Billing and financial statements
- Coding sheets
- Duplicate or recurring invoices
- General ledgers
- Expense reports
- Revenue recognition documents
- Bonus or incentive plan documents
- Appeal/Denial packets
- Documents you reasonably believe relate to the claims at issue

Clinical & Medical Necessity Records

Documents showing what care was actually provided

- Patient health records
- Physician orders
- Lab test orders
- Prior authorization files
- Utilization review reports
- Supply usage logs

Whistleblower Evidence

Contemporaneous Notes

When you observe a relevant event, take concise, detailed, and dated notes as soon as possible. Describe what you saw or heard, who was present, and any other pertinent details you wish to share with your lawyer.

Recordings

Recordings of meetings and conversations can provide useful evidence, as long as the recordings are legal. Before you record a meeting or conversation you are participating in, know whether all participants are in one-party or two-party consent states. Most states have made it illegal to secretly record a conversation in which you are not a participant. Some routine business recording systems—such as voicemail, call logs, and security footage—might be available in discovery; make note of those systems when they might have preserved relevant evidence. You can retain, and share, voicemails left for you.

Email Correspondence

Relevant email communications that come your way during your work, including those received through a listserv, are valuable evidence of an organization’s actual functioning. But don’t send probing or misleading messages for the sake of gathering evidence.

Face-to-Face Conversations

Use contemporaneous notes to preserve regular workplace interactions that are relevant to the fraud or to claims regarding retaliation. But don’t use face-to-face conversations to generate evidence—avoid encouraging colleagues to repeat statements, express opinions, or “confirm” misconduct.

Timeline

Create a timeline of the fraudulent activity from when you first observed it to the most recent occurrence. Make sure to document any attempts you made to alert supervisors or compliance teams, as well as any involvement you may have had with the false claims.

Witness List

Make lists of everyone you think may have knowledge of the fraud. Record names, positions and responsibilities, and what you think the person will know. Note whether the witness would likely be cooperative and provide as much contact information as you have.

HIPAA & Patient Records

You can legally share patient records or relevant patient information with your attorney or authorized government investigators when reporting suspected fraud. HIPAA allows disclosures made to expose wrongdoing, as long as you only access information through your normal job duties. Proper whistleblower reporting is fully protected under federal privacy rules.