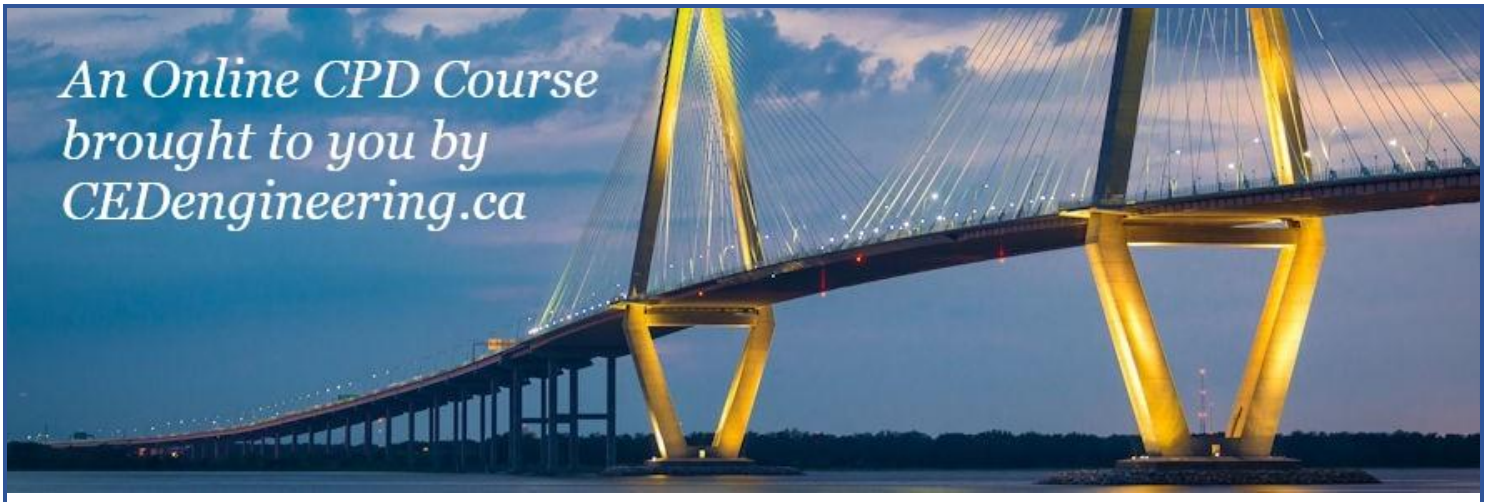

Data Integrity For Professional Engineers

Course No: LE2-029
Credit: 2 PDH

Jeelan Moghraby, PhD., MBA

Continuing Education and Development, Inc.

P: (877) 322-5800
info@cedengineering.ca

Table of Contents

Module 1: Foundations of Research and Data Integrity in Engineering Practice 1

1.1 Introduction..... 1

1.2 The Federal Framework for Research Misconduct..... 1

1.3 Honest Error, Negligence, and Intentional Misrepresentation..... 2

1.4 Integrity, Public Safety, and Professional Standing..... 3

Module 2: Integrity Across the Engineering Data Lifecycle 5

2.1 The Stages and Their Characteristic Risks 5

2.2 Defensible Records and Traceability 6

2.3 Certified Data and the Chain of Reliance 7

Module 3: Misrepresentation, Misconduct, and the Pressures Behind Them 9

3.1 The Forms Misrepresentation Takes 9

3.2 The Pressures That Drive It 10

3.3 The Quantitative Anatomy of a Small Manipulation..... 11

Module 4: Professional Obligations, Safeguards, and Response 13

4.1 What the Codes and Rules Require 13

4.2 Building Integrity into Practice 14

4.3 Responding to a Suspected Data-Integrity Problem..... 15

Course Summary..... 17

References 18

Appendix A: Glossary of Key Terms 19

Appendix B: Disciplinary Case Studies..... 20

Case 1: Fraudulent or deceitful written assertions (Texas)..... 20

Case 2: Misrepresenting responsible charge through sealing (Texas)..... 20

Case 3: Negligence in sealed engineering work (Florida)..... 21

Module 1: Foundations of Research and Data Integrity in Engineering Practice



1.1 Introduction

Engineering rests on information that someone collected, recorded, analyzed, and represented as accurate. Two ideas frame this course, and each carries a specific meaning in engineering practice: what is data integrity and why does so much engineering work qualify as research.

Data integrity signifies that the engineering information is complete, accurate, and traceable to the conditions under which it was produced. It covers the measurements an engineer records in the field, the results a laboratory reports, the calculations behind a design, and the assertions an engineer signs and seals. When that information remains valid, the decisions built on it are reliable and justified. When it is altered, selectively reported, or invented, every downstream decision inherits the flaw, often silently, until a structure, system, or product behaves in a way the records said it would not. The integrity of engineering data is, in this sense, inseparable from the integrity of engineering itself.

The word **research** can mislead engineers who associate it only with universities and journals. In practice, the activities that generate engineering data are research activities, such as qualifying a material, characterizing a soil, running an emissions or efficiency test, reconstructing a failure, validating a model against measured behavior. Each produces evidence that others will rely on without repeating the work. The standards that govern honest research, accurate recording, faithful reporting, and clear attribution apply just as strictly to engineering work, and the consequences of breaching them tend to be more immediate than in academic settings, because the output is built, operated, or relied upon by the public.

1.2 The Federal Framework for Research Misconduct

United States policy defines research misconduct through a single framework that has shaped how every regulated field, including engineering disciplines that receive federal funding, understands the boundaries of acceptable practice. The federal research misconduct policy, issued by the Office of Science and Technology

© Dr Jeelan Moghraby, 2026

Policy, defines misconduct as "fabrication, falsification, or plagiarism in proposing, performing, or reviewing research, or in reporting research results" (Office of Science and Technology Policy, 2000). The Public Health Service codified the same three categories in regulation (42 C.F.R. § 93, 2005). Together these three categories are commonly referred to as FFP (see Table 1).

The framework draws two distinctions that matter to engineers. First, the misconduct must be a significant departure from accepted practices, and it must be committed intentionally, knowingly, or recklessly. Honest error and good-faith differences of scientific or engineering judgment fall outside this definition. An engineer who reaches a defensible but later disproven conclusion has not committed misconduct, however, an engineer who alters the underlying data to reach a desired conclusion has. Second, the burden of distinguishing the two rests on a documented record. Where records are thin, an honest engineer and a dishonest one can look alike, which is one reason traceable data practices matter as much as honest intent.

Table 1. Fabrication, falsification, and plagiarism, and their engineering forms

Category	Definition	How it appears in engineering practice
Fabrication	Making up data or results and recording or reporting them.	Reporting test results for samples that were never tested; inventing field measurements; creating an inspection record for a visit that did not occur.
Falsification	Manipulating research materials, equipment, or processes, or changing or omitting data such that the record does not accurately reflect the work.	Editing instrument output; excluding inconvenient results without basis; altering calibration records; tuning a test so the article passes only under test conditions.
Plagiarism	Appropriating another person's ideas, results, or words without giving appropriate credit.	Submitting another firm's calculations or report as one's own; reusing a colleague's analysis without attribution; sealing work prepared by an unlicensed or uncredited author.

Note: Definitions adapted from Office of Science and Technology Policy (2000) and 42 C.F.R. § 93 (2005).

1.3 Honest Error, Negligence, and Intentional Misrepresentation

The federal framework excludes honest error and good-faith differences of judgment, but practicing engineers need a finer distinction, because boards, clients, and courts treat three things very differently: honest error, negligence, and intentional misrepresentation. The three can produce the same wrong number on a page, yet they carry different culpability and different consequences and confusing them leads engineers either to excuse misconduct as a mistake or to brand a defensible judgment as fraud.

Honest error is a wrong result reached in good faith using accepted methods, the kind of mistake that careful review is meant to catch and that the record shows was made openly. Examples can be a transposed digit caught and corrected, a model assumption that proved conservative, or an early estimate later refined. None of these are an integrity failure, provided the work was done in good faith and the record reflects what happened.

Negligence is a failure to exercise the care a competent engineer would exercise, producing work that falls below the standard of practice. It does not require intent to deceive as the engineer who seals a deficient analysis because they did not check it has been negligent, regardless of whether they believed it was correct or not.

Intentional misrepresentation is the knowing or reckless distortion of the record; an engineer who alters, omits, or invents data, or who reports a result they know the data does not support.

Table 2 distinguishes between these three, and how a board might judge them. Only intentional misrepresentation is research misconduct in the federal sense, but all three can result in board discipline, and negligence is in fact the most common basis for disciplinary action against engineers.

Table 2. Distinguishing honest error, negligence, and intentional misrepresentation

Category	What it is	State of mind	Typical professional consequence
Honest error	A wrong result reached in good faith using accepted methods, openly recorded.	No intent to deceive; ordinary fallibility.	Correction; generally no discipline where the record shows good faith.
Negligence	Work falling below the standard of care a competent engineer would exercise.	No intent to deceive, but inadequate care.	Board discipline (fine, probation, required education); the most common basis for action.
Intentional misrepresentation	Knowing or reckless distortion, omission, or invention of data or results.	Intent to deceive, or reckless disregard for truth.	Suspension or revocation; possible civil or criminal liability; research misconduct.

In practice, the line between negligence and misrepresentation is where most of the disputes are, and the deciding factor is usually the record. An engineer who documented an outlier exclusion, stated the basis at the time, and reported it openly has a defensible position even if the judgment is later questioned. An engineer who quietly dropped the same value and left no trace will appear to a reviewer indistinguishable from one who concealed it, because the documentation that would have separated the two does not exist. Documentation practices are what allows an honest engineer to prove honesty when a result is challenged.

1.4 Integrity, Public Safety, and Professional Standing

For a licensed engineer, data integrity is not one obligation among many; it sits beneath the obligation that the profession ranks first. The NSPE Code of Ethics opens with the requirement that engineers hold paramount the safety, health, and welfare of the public, and it separately requires that engineers issue public statements only in an objective and truthful manner and avoid deceptive acts (National Society of Professional Engineers, 2019). Each of these duties depends on the data underneath it. An engineer cannot protect the public using a

design grounded in falsified soil data, and an engineer cannot make a truthful statement about a product while concealing the test that contradicts it. Figure 1 shows how the duty of data integrity supports the higher duties rather than competing with them.

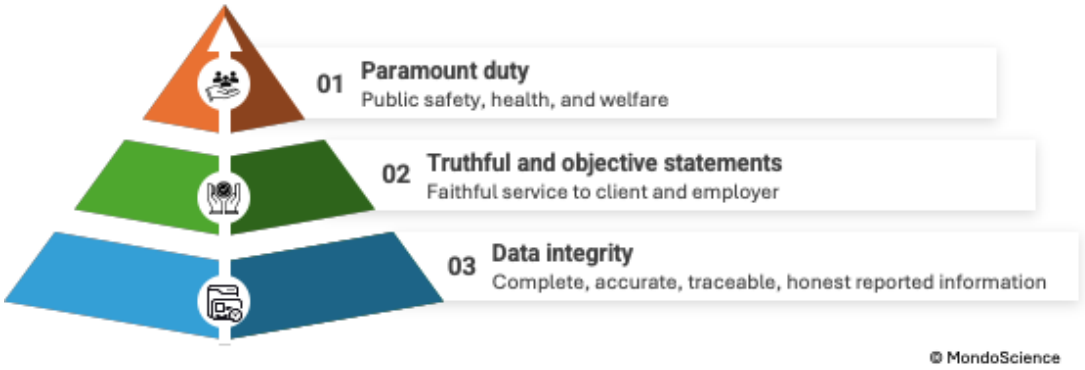

Figure 1. Data integrity as the foundation of the engineer's hierarchy of professional obligation

The Volkswagen diesel emissions case is an example of how the loss of data integrity propagates upward through the hierarchy illustrated in Figure 1. In about 2006, a group of Volkswagen engineers set out to design a diesel engine that would meet stringent United States nitrogen oxide standards. When they concluded they could not meet those standards within the performance and cost limits the company wanted, they designed software that detected when a vehicle was undergoing laboratory emissions testing and activated full emissions controls only during the test (U.S. EPA, 2015). On the road, the same vehicles emitted nitrogen oxide at many times the legal limit. The data the company submitted to regulators was, by design, not representative of how the vehicles actually behaved.

This case is instructive because the falsification was technically sophisticated and the people who built it were capable engineers. One of them, James Liang, pleaded guilty in United States federal court to conspiracy and was sentenced to a prison term and a fine for his role. A compliance executive, Oliver Schmidt, received a longer sentence, and the company itself pleaded guilty and agreed to criminal and civil penalties measured in billions of dollars (U.S. Department of Justice, 2017). The engineers did not set out to harm anyone. They set out to close a gap between what the product could do and what the records needed to say, and they closed it by corrupting the data rather than by reporting the shortfall.

The professional cost is as durable as the legal one. A licensed engineer found to have falsified or misrepresented data faces board discipline that becomes part of a permanent, publicly searchable record, and that discipline frequently follows the engineer across state lines through reciprocal action (see Chapter 4 and Appendix C). Restoring a damaged design is often possible, but restoring a damaged professional reputation rarely is.

Module 2: Integrity Across the Engineering Data Lifecycle

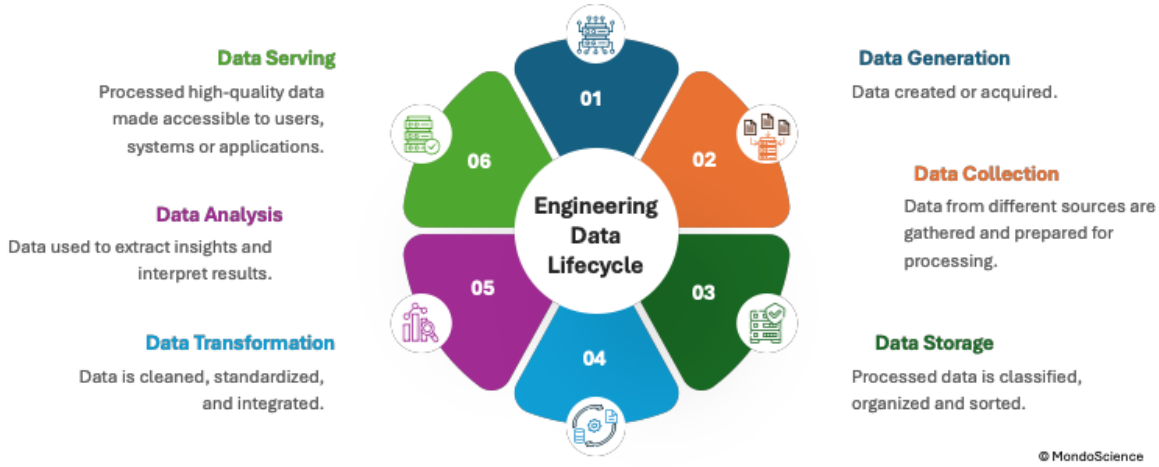

Figure 2. General engineering data lifecycle

Engineering data has a lifecycle (see Figure 2). Data is collected, recorded, analyzed, retained, and reported, and at each transition it can be corrupted, degraded, or lost. Treating integrity as a single event, a yes-or-no question asked once at the end, misses most of the risk, because the opportunities to compromise data are distributed across its whole life. Early compromises are the hardest to detect. For example, a sound analysis built on a quietly edited input will produce a confident but wrong answer. This chapter follows the engineering data lifecycle stage by stage and identifies where integrity is most exposed at each one.

2.1 The Stages and Their Characteristic Risks

Each stage of the lifecycle carries a characteristic risk, one that follows from what the stage does rather than from carelessness in general. Identifying the risk at each stage is what makes it controllable, because a risk that has not been identified has no owner and no control assigned to it.

The five stages described below are set out in the order the data passes through them, with the risk that belongs to each (see Figure 3).

Collection is where data enters the record from the physical world, through a gauge, a sensor, a sample, or an observation. The characteristic risk is that the conditions of collection are not captured, for example, the instrument that was out of calibration, the sample taken from the wrong location, the reading recorded from memory an hour later.

Recording is the act of committing the observation to a durable medium. Its risk is transcription and the temptation to tidy. For example, rounding as one writes, dropping a digit, or recording the value that was expected rather than the value observed.

Analysis transforms recorded data into results, and its risks are selective processing, the undocumented exclusion of data points, and the choice of a method after seeing which method gives the preferred answer.

Retention preserves the record for the period others may need it, and its risk is silent loss, overwriting, or the absence of any version history.

Reporting communicates results to those who will rely on them, and its risks are omission, misleading presentation, and assertions that outrun the evidence.

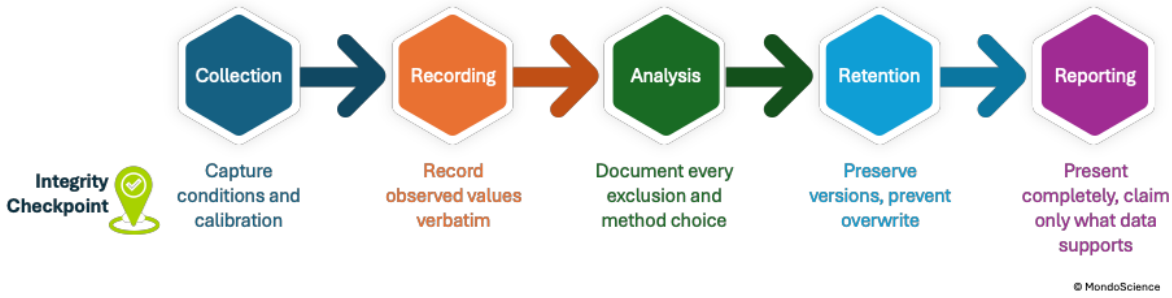

Figure 3. Stages of data lifecycle with their integrity checkpoint

In practice, the distinction between stages is easy to overlook because a single engineer often performs several of them in one sitting. The value of separating them is that each stage suggests a different control, for example:

- Calibration logs protect collection
- Verbatim recording and the absence of deletion protect recording
- Documented analytical decisions protect analysis
- Version control protects retention
- Complete, qualified reporting protects the final step

An organization that relies on a single end-of-process review to catch every problem is depending on the least effective control at the latest possible moment.

2.2 Defensible Records and Traceability

A **defensible record** is one that lets an outside engineer reconstruct what was done, by whom, when, and under what conditions, and reach the same result from the same inputs. This is the working definition of traceability, and it is the difference between data that can be defended before a board or a court from data that cannot. The international standard for testing and calibration laboratories, ISO/IEC 17025, builds much of its requirements around this idea. Records must be retained, contemporaneous, attributable, and protected against unauthorized amendment, and any change must be traceable to the previous version (ISO, 2017).

Engineers who never set foot in an accredited laboratory still benefit from adopting its record discipline, because the questions a record must answer are the same in any setting. Table 3 below lists the elements of a

defensible engineering data record aligned with the record-control principles of ISO/IEC 17025 (ISO, 2017). The difficulty lies in maintaining them consistently when schedules are tight and the work feels routine.

Table 3. Elements of a defensible engineering data record

Element of a defensible record	What it establishes	Common failure
Attribution	Who collected, recorded, or analyzed the data.	Unsigned field notes; shared logins that mask who entered a value.
Contemporaneity	That the record was made at the time of the work.	Notes written up days later from memory; back-dated entries.
Original values preserved	That observed values were not overwritten.	Erased or typed-over readings with no trace of the original.
Conditions captured	Calibration status, environment, sample identity, method.	Results reported with no link to the instrument or its calibration record.
Version traceability	That any change can be traced to its prior state and author.	Files overwritten in place; no change history; ambiguous "final_v2" copies.
Retention	That the record survives for the period others may rely on it.	Records discarded or lost before the audit or design life requires.

These elements are often summarized by the acronym **ALCOA**, which holds that data should be **attributable**, **legible**, **contemporaneous**, **original**, and **accurate**. This acronym is useful because it applies as well to a field notebook as to a database. The shift to electronic records has not changed the principles. An electronic record is defensible only if the system carries an audit trail that captures who changed what, when, and why, and that cannot be silently overwritten. A spreadsheet emailed back and forth, edited in place by several people with no version history, fails this test even when every individual entry is honest, because the record cannot answer the questions a defensible record must answer. Engineers increasingly inherit data from instruments and software they did not configure, and part of professional diligence now includes confirming that those systems preserve original values and log changes rather than assuming they do.

2.3 Certified Data and the Chain of Reliance

Much of engineering data is consumed far from where it is produced, by people who cannot inspect the work and must trust the certificate. For example, a certified material test report travels with a steel shipment; a calibration certificate accompanies an instrument; a sealed geotechnical report informs a foundation designed by someone who never saw the borehole. This chain of reliance is efficient, but it is fragile because a falsification at the source contaminates every party downstream who had no way to detect it.

The Kobe Steel case illustrates the reach of a single corrupted source. In 2017 the Japanese steelmaker admitted that employees had falsified data on the strength, durability, and dimensions of aluminum, copper,

and steel products, in some cases altering inspection certificates so that products that did not meet customer specifications appeared to pass (Reuters, 2018). Investigations traced the practice across more than twenty plants and, by the company's own account, went back several decades. The falsified certificates flowed into the supply chains of automakers, aircraft and train manufacturers, and defense and aerospace producers worldwide. In the United States, the Nuclear Regulatory Commission examined whether falsified Kobe Steel material certificates had entered safety-related nuclear construction, identifying specific components supplied with certified material test reports that required independent verification (U.S. Nuclear Regulatory Commission, 2018).

The practical question for the engineer who receives third-party data is how much verification the application demands. The honest answer is that it scales with consequence. For low-consequence work, a current certificate from a qualified supplier may reasonably be accepted at face value. For work where failure threatens safety, the standard of care rises to include spot-check testing, independent verification, supplier audits, and traceability back to accredited laboratories as part of diligent practice. The Kobe Steel case highlights how the falsified certificates were, on face value, ordinary and complete; nothing in the paperwork signaled the problem. An engineer cannot detect a well-executed falsification by reading the certificate. This reinforces the need for building verification into the process for critical applications.

The following two lessons are important to understand for any practicing engineer. The first is that a certificate is only as trustworthy as the integrity culture of the party that issued it. This is why qualification, audit, and, for critical applications, independent verification exists. An engineer who treats every certificate as self-evidently true has delegated a safety judgment to a stranger. The second is the position of the engineer who issues the certificate. Each falsified Kobe Steel report was signed by someone, and each signature placed an individual's professional credibility behind a number known to be false. The certificate is the point at which the data lifecycle and personal accountability meet.

© Dr Jeelan Moghraby, 2026

Module 3: Misrepresentation, Misconduct, and the Pressures Behind Them

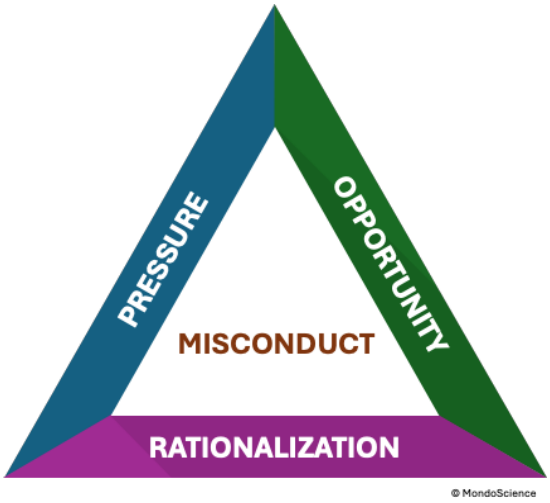

Figure 4. Misconduct triangle

Most engineers will never fabricate a data set outright. Far more will face the smaller decisions on whether to mention the one cylinder that broke below strength, whether to round a value that lands just outside a limit, or whether to present a chart in the way that flatters the result. These choices rarely announce themselves as misconduct, which is what makes them dangerous. This chapter sets out the different forms misrepresentation takes, the pressures that make competent people choose it, and the quantitative anatomy of a manipulation small enough to feel defensible yet large enough to change a conclusion.

3.1 The Forms Misrepresentation Takes

Misrepresentation runs from the blatant to the barely perceptible, the latter of which cause the most problems because they are easy to rationalize and hard to detect. Table 4 below sets out the recurring forms of misrepresentation and how each manifest in engineering data.

Table 4. Recurring forms of data misrepresentation in engineering practice

Form	How it manifests
Outright fabrication	Reporting results for work never performed, such as inspections not conducted or samples not tested.
Selective exclusion	Dropping data points that conflict with the desired result without a stated, pre-defined basis.
Method shopping	Choosing the analysis, model, or acceptance test after seeing which one yields the preferred answer.
Misleading presentation	Truncated or shifted axes, suppressed baselines, or aggregation that hides the variation that matters.
Omission	Reporting the favorable results completely while leaving out an unfavorable test or condition.
Boundary rounding	Rounding or truncating a value specifically to move it across a specification limit it would otherwise miss.

3.2 The Pressures That Drive It

Understanding why capable engineers misrepresent data is a prerequisite for guarding against it, because the pressures are structural and predictable. For example, the Volkswagen case described in Chapter 1 began with a gap the engineers could not close honestly within the constraints they were given, combined with a schedule and a market commitment that treated failure as unacceptable. When an organization commits publicly to a result before confirming it can be achieved, it converts a technical shortfall into a reputational crisis, and the pressure to make the data conform grows with each step the commitment advances.

Three pressures appear again and again:

- **Schedule pressure** makes the time to redo a test or investigate an anomaly feel unavailable, so the anomaly is quietly dropped.
- **Commercial and competitive pressure** attaches a price to every failed result, whether a missed delivery, a lost contract, or a product that cannot ship, and that price is paid by the person holding the inconvenient number.
- **Career pressure** operates at the individual level: the engineer who reports the failure may be blamed for it, while the engineer who makes it disappear is, in the short run, rewarded.

Layered over all three is **normalization**, the process by which a small deviation, once tolerated, becomes the baseline against which the next, slightly larger deviation is judged. Kobe Steel's falsification reportedly persisted across decades and plants because it had become ordinary; no single employee felt that they were starting a fraud (Reuters, 2018).

The sociologist Diane Vaughan described the normalization of deviance as the process by which a group gradually comes to accept a departure from a standard as normal, each small acceptance lowering the threshold for the next, until conduct that would once have been recognized as unacceptable becomes routine and invisible to those inside the system (Vaughan, 1996). For data, this is how a single tolerated exclusion becomes a habit, and a habit becomes a culture. An engineer who joins such an organization rarely confronts a clear choice to commit fraud; they confront a settled practice that everyone around them treats as ordinary, which is a far more difficult to resist.

This pattern also recurs across firms, which argues against treating any one case as an aberration. In the years surrounding the Volkswagen disclosures, United States and European authorities pursued similar emissions-data matters at other manufacturers. A Fiat Chrysler diesel engineer was charged in connection with software alleged to have concealed emissions behavior, and the company later resolved related criminal and civil claims (U.S. Department of Justice, 2017). Several major manufacturers in the same period acknowledged falsified quality or inspection data of various kinds. That the same conduct appeared independently at multiple capable organizations indicates that the driver is structural, the predictable response to a gap between committed performance and achievable performance, rather than the failing of a few individuals.

As regulators closed in, a Volkswagen employee, in a meeting at which the agreed corporate script called for continued concealment, departed from that script and disclosed to the California Air Resources Board that the vehicles contained software designed to defeat the emissions test (EPA, 2018). The same structure that produced years of falsification also contained the individual decision that ended it. Pressure shapes behavior; it does not fully determine it, and the engineer retains the choice

3.3 The Quantitative Anatomy of a Small Manipulation

The reason boundary manipulations succeed is that, when viewed in isolation, each looks like an ordinary engineering judgment. The following hypothetical illustration, which uses invented numbers chosen for clarity, shows how a single excluded value changes a conformance decision.

Suppose acceptance of a concrete pour depends on the average compressive strength of a set of test cylinders meeting a specified minimum of 4,000 psi (27.6 MPa). Seven cylinders are tested, with results of 4,350, 4,210, 4,180, 4,090, 3,980, 4,260, and 3,540 psi.

The mean of all seven values is approximately 4,087 psi, above the specified minimum (see Figure 5), but the spread and the single low result of 3,540 psi would ordinarily prompt investigation into why one cylinder fell so far below the others.

The engineer under pressure to accept the pour might be tempted to discard the 3,540 psi result as an outlier without a documented basis. Excluding it raises the reported mean of the remaining six to approximately 4,178 psi and removes the very evidence that should trigger scrutiny (see Figure 5).

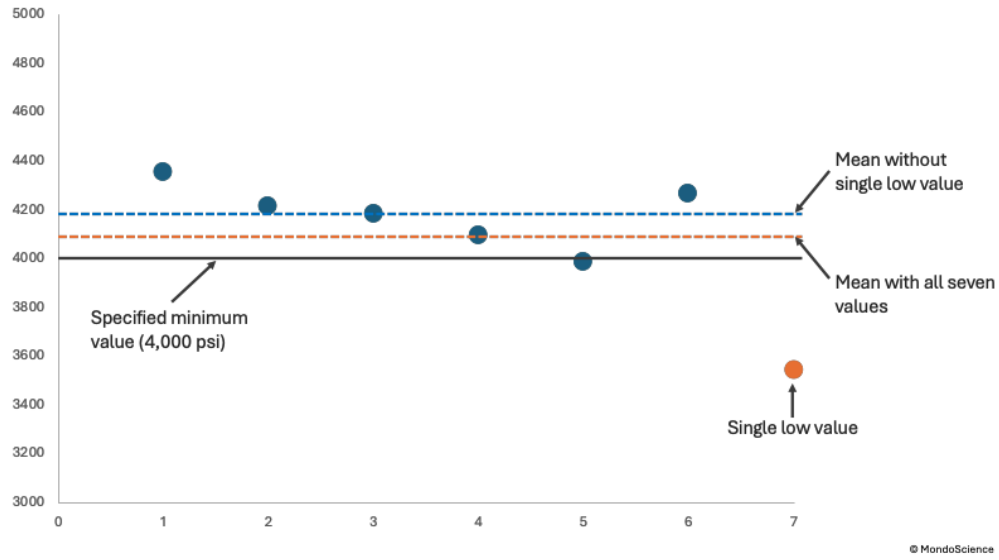

Figure 5. Illustrative effect of undocumented outlier exclusion on a conformance decision

The integrity question is whether the exclusion follows a defined rule applied before the results were seen, or whether it follows the desire for a particular answer. A legitimate outlier procedure is defined in advance and documented; an exclusion chosen to clear a limit is falsification, regardless of how reasonable the discarded value looks once it is gone.

Graphical presentation offers the same opportunity for a technically accurate distortion. A chart whose vertical axis begins not at zero but just below the lowest data point can turn a negligible variation into a dramatic trend, or flatten a meaningful change into apparent stability, without altering a single underlying number. For example, a series of monthly measurements varies between 98 and 102 against a target of 100. Plotted on an axis running from 0 to 120, the data looks flat and stable; plotted on an axis running from 97 to 103, the same data looks volatile and alarming. Neither chart contains a false value, yet they support opposite conclusions, and the engineer who selects the axis to produce the impression they want has misrepresented the data as surely as one who altered it. The defense is the same as for rounding and exclusion: choose the presentation convention to serve clarity, fix it before the conclusion is known, and disclose the scale so the reader can judge the variation for themselves.

Rounding produces the same kind of quiet shift. A measured value of 3,996 psi against a 4,000 psi minimum fails, while if it is reported as "4,000 psi" after rounding to the nearest hundred, it appears to pass. Engineering practice anticipates this by fixing the rounding convention before conformance is assessed rather than after. ASTM E29 provides a standard method for using significant digits in test data to determine conformance with specifications, including the rounding rule and the point at which it is applied, so that the decision does not turn on a convenient choice made with the limit in view (ASTM International, 2013). A rounding convention, an outlier rule, or an acceptance criterion is a safeguard when fixed in advance and a manipulation when selected to produce a wanted result. The decisions in this chapter are where a routine analytical choice becomes an ethical one, and where the safeguards in the final chapter do their work.

Module 4: Professional Obligations, Safeguards, and Response

An engineer's obligations regarding data are not left to personal conscience alone. They are written into the codes of ethics the profession adopts and into the rules every state licensing board enforces, and they carry consequences that reach the license itself. This chapter maps those obligations onto everyday data handling, describes the safeguards that make honest practice the default, and sets out how to respond, and how to document a response, when data appears to have been compromised.

4.1 What the Codes and Rules Require

The NSPE Code of Ethics states the duties most directly relevant to data in a small number of provisions. Engineers are to hold the public's safety, health, and welfare paramount; to issue public statements only in an objective and truthful manner and to include all relevant and pertinent information in professional reports; to act as faithful agents for clients and employers; and to avoid deceptive acts (NSPE, 2019). Table 5 restates these in terms of concrete data obligations.

Table 5. NSPE Code provisions mapped to concrete data obligations

Code provision (paraphrased)	Concrete data obligation
Hold paramount public safety, health, and welfare (Fundamental Canon 1).	Do not let a desired result override data that bears on whether something is safe; treat a suppressed safety-relevant result as a paramount-duty failure.
Issue statements only in an objective and truthful manner (Fundamental Canon 3).	Report what the data shows, including unfavorable results; do not present partial data as if it were complete.
Include all relevant and pertinent information in reports (Prof. Obligation).	Disclose excluded data points, deviations, and the conditions and methods used; let the reader see what was set aside.
Act as a faithful agent or trustee (Fundamental Canon 4).	Serve the client's genuine interest in correct results, which is never served by data the client cannot rely on.
Avoid deceptive acts (Fundamental Canon 5).	Treat misleading presentation, convenient rounding, and method shopping as deception even when each value reported is technically a number that was produced.

Note: Provisions paraphrased from National Society of Professional Engineers (2019). The provision references are given for reference and should be confirmed against the current published Code.

In addition to the NSPE Code of Ethics, there are the discipline-specific codes reinforcing the same data obligations from their own vantage points. The ASCE Code of Ethics directs civil engineers to be objective and truthful and to report work that conforms to applicable standards, and the codes of ASME, IEEE, and AIChE carry parallel duties of honesty in the presentation of data and conclusions (American Society of Civil Engineers, 2020). An engineer who holds membership in a technical society is bound by that society's code

in addition to the board's rules. The codes are written to converge rather than conflict; the obligation to report data honestly appears in every one of them. Where they differ is mainly in emphasis and in the specific procedures for raising concerns, which is why it is important for engineers to know the specific code that governs their practice.

State boards convert these duties into enforceable rules. The NCEES Model Rules, which most state boards draw on, require licensees to be objective and truthful in professional reports and statements, and to express conclusions only where supported by adequate knowledge (NCEES, 2025). The board cases in Appendix C show how these rules are applied in practice, where engineers are disciplined for fraudulent or misleading written assertions, for sealing work that misrepresented who performed it, and for negligent work that the sealed record presented as sound.

4.2 Building Integrity into Practice

Safeguards work best when they are built into the workflow rather than applied as a final inspection. Control that depends on a tired engineer remembering to be honest at the end of a long project is the weakest kind. The most effective measures make the honest path the path of least resistance. Defining analytical decisions in advance is the single most powerful safeguard against boundary manipulation: an outlier rule, a rounding convention, and an acceptance criterion all fixed before results are seen remove the opportunity to choose the method that gives the desired answer. ASTM E29 serves this purpose for conformance rounding, and pre-registered acceptance procedures serve it for testing programs (ASTM International, 2013).

Independent review supplies a second control. A second qualified engineer who checks not only the conclusion but the data behind it, including what was excluded and why, catches both error and the early forms of misrepresentation while they are still correctable. Version-controlled records supply a third form of control. When every change to a data file is traceable to its author and prior state, silent editing becomes visible, and the difference between a corrected transcription error and a falsification becomes a matter of record rather than of memory. Contemporaneous recording, retention for the full period others may rely on the data, and clear separation of raw observations from processed results complete the set. None of these is costly to maintain once established, yet all of them are expensive to reconstruct after a dispute, when their absence is what the inquiry will note.

Practical test for a data decision*: Before excluding a value, choosing a method, or selecting how to present a result, ask whether the same decision would have been made if the result had come out the other way, and whether the basis for it was fixed before the data was seen. A decision that survives both questions is defensible; one that fails either leads to misrepresentation.*

Safeguards also operate at the level of culture, and culture is set by what leaders reward. An organization that treats every reported failure as a problem to be solved, rather than a person to be blamed, removes much of the pressure that drives concealment. For the individual engineer, the practical defense is to make integrity habitual rather than heroic by writing down the basis for a judgment when it is made, keeping raw data separate from processed results, and by treating the question "could I defend this decision to a board?" as a

routine part of the work, rather than a question asked only when something has gone wrong. Habits formed in ordinary work are what hold under pressure.

4.3 Responding to a Suspected Data-Integrity Problem

An engineer who suspects that data has been fabricated, falsified, or misrepresented faces a sequence of decisions, and handling them well protects both the public and the engineer (see Figure 6).

- Step 1 is to preserve the record: secure the original data, files, and correspondence before anything can be altered, because the difference between a substantiated concern and an unprovable suspicion is usually the documentation.
- Step 2 is to verify before alleging: confirm that the discrepancy is not honest error or a difference of method, since a misconduct allegation is serious and a premature one can do real harm.
- Step 3 is to raise the concern internally through the appropriate channel, in writing, keeping a dated copy, so that the act of raising it is itself part of the record.

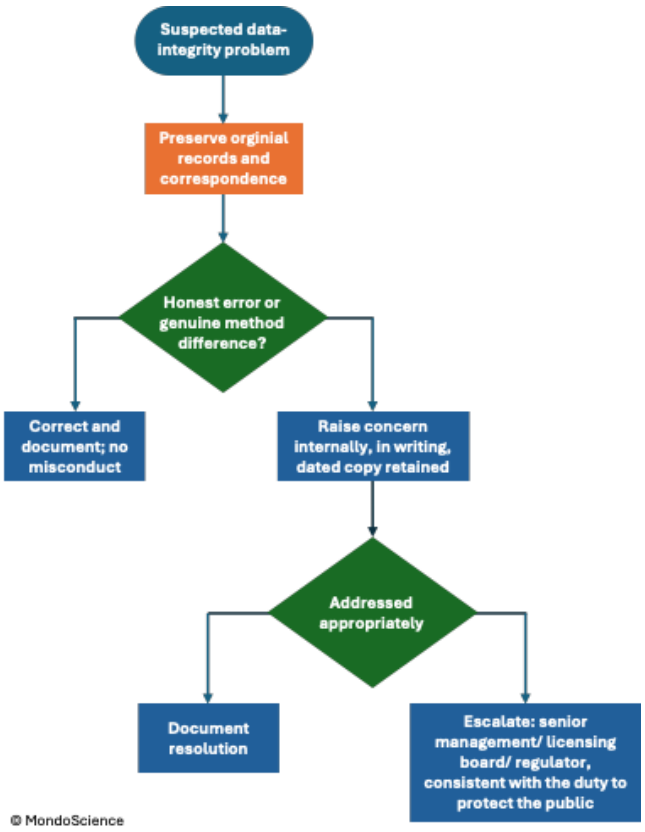

Figure 6. A decision pathway for responding to a suspected data-integrity problem

Documenting the concern matters as much as raising it. An engineer who reports a suspected problem verbally and is later overruled has little to show for it. However, if they had put the concern in writing, described the specific data and why it troubled them, and retained a dated copy, has created a record that protects both the public interest and their own position.

Where the situation is genuinely unclear, seeking confidential guidance, from a trusted senior colleague, a professional society's ethics resources, or independent counsel, is itself part of acting diligently rather than a sign of indecision. Engineers should also be realistic about the personal cost: raising integrity concerns can strain relationships and careers, which is precisely why the obligation is written into the codes rather than left to individual courage. The protections available to those who report vary by employer and jurisdiction, and an engineer weighing escalation is entitled to understand them before acting.

If the concern is not addressed internally, the engineer's paramount duty to the public can require escalation beyond the organization, to a client, a licensing board, or a regulator, depending on the risk involved. This is the hardest step, and the Volkswagen disclosure to the California Air Resources Board shows both its difficulty and its effect: a single employee's decision to depart from the concealment script is what finally exposed the scheme to regulators (EPA, 2018). The NSPE Code of Ethics frames disclosure as an obligation rather than an option where the public safety, health, or welfare is endangered, and most state boards require licensees to report knowledge of violations through defined channels (NSPE, 2019).

Data integrity is a continuous professional practice and is protected by the records an engineer keeps at the bench, the analytical rules fixed before results are seen, the review a colleague performs, and the willingness to report a result honestly when an honest result is unwelcome. The engineers in the cases described in this course were capable people who, at a specific moment, let a desired record displace an accurate one. The obligations and safeguards set out in this chapter exist so that, at such a moment, the accurate record is the one that prevails.

Course Summary

Research and data integrity is the discipline of ensuring that engineering information is produced, recorded, analyzed, retained, and reported honestly and accurately, so that the people who rely on it can trust what it says. It rests on a federal framework that defines research misconduct as fabrication, falsification, and plagiarism, while deliberately excluding honest error and good-faith differences of judgment. For licensed engineers, the profession's paramount duty to public safety, its requirement of truthful statements, and its prohibition on deceptive acts all depend on the data beneath them. When the data is corrupted, those higher duties fail with it.

The risk to integrity is distributed across the whole life of the data, from collection through reporting, and the earliest compromises are the hardest to detect later on. Defensible records, attributable, contemporaneous, traceable, and retained, are what let a competent outside engineer reconstruct the work and reach the same result; they are what distinguish data that can be defended from data that cannot. Because much engineering data is consumed far from where it is produced, through certificates and sealed reports, a single falsification at the source can contaminate every party downstream, as the Volkswagen and Kobe Steel cases demonstrated on an international scale.

Misrepresentation runs from outright fabrication to boundary rounding and selective exclusion that feel like ordinary judgment. Competent engineers reach for these under predictable pressures of schedule, commerce, and career, amplified by the normalization of small deviations over time. The defense is structural: fix analytical decisions before results are seen, subject data to independent review, keep version-controlled records, and report results honestly even when they are unwelcome. When a problem is suspected, the engineer preserves the record, verifies before alleging, raises the concern in writing, and escalates where the public is at risk.

Key Takeaways

- Data integrity underlies the engineer's paramount duties; falsified data defeats the duty to protect the public before any design decision is made.
- Research misconduct is defined as fabrication, falsification, or plagiarism committed intentionally, knowingly, or recklessly; honest error and good-faith judgment differences are excluded.
- Integrity is lost across the data lifecycle, not at a single checkpoint; controls belong at every stage, not only at final review.
- A defensible record is attributable, contemporaneous, original-value-preserving, condition-capturing, version-traceable, and retained.
- Boundary manipulations succeed because each looks like ordinary judgment; the test is whether the basis was fixed before the result was seen and would hold if the result had been reversed.
- The strongest safeguards make the honest path the default: pre-defined methods, independent review of the data itself, and version control.
- When integrity is in question, preserve records, verify before alleging, raise concerns in writing, and escalate to protect the public where necessary.

References

1. American Society of Civil Engineers. (2020). *Code of ethics*. ASCE. https://www.asce.org/career-growth/ethics/code-of-ethics

2. ASTM International. (2013). *Standard practice for using significant digits in test data to determine conformance with specifications (ASTM E29-13)*. ASTM International.

3. Code of Federal Regulations. (2005). *Public Health Service policies on research misconduct*, 42 C.F.R. § 93.

4. International Organization for Standardization. (2017). *General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025:2017)*. ISO.

5. National Council of Examiners for Engineering and Surveying. (2025). *Model rules*. NCEES.

6. National Society of Professional Engineers. (2019). *NSPE code of ethics for engineers*. NSPE. https://www.nspe.org/resources/ethics/code-ethics

7. Office of Science and Technology Policy. (2000). *Federal policy on research misconduct*. Federal Register, 65(235), 76260–76264.

8. Reuters. (2018, March 6). *Kobe Steel admits data fraud went on nearly five decades, CEO to quit.* Reuters.

9. United States Department of Justice. (2017). *Volkswagen AG agrees to plead guilty and pay $4.3 billion in criminal and civil penalties; six Volkswagen executives and employees indicted in connection with conspiracy to cheat U.S. emissions tests*. Press release. https://www.justice.gov/opa/pr

10. United States Environmental Protection Agency. (2015). *Notice of violation of the Clean Air Act to Volkswagen AG, Audi AG, and Volkswagen Group of America, Inc*. EPA.

11. United States Environmental Protection Agency. (2018). *Former CEO of Volkswagen AG charged with conspiracy and wire fraud in diesel emissions scandal*. News release. EPA. https://www.epa.gov/archive/epa/newsreleases

12. United States Nuclear Regulatory Commission. (2018). *Kobe Steel quality assurance record falsification* (ADAMS Accession No. ML18190A466). NRC.

13. Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. University of Chicago Press.

Appendix A: Glossary of Key Terms

Term	Definition
Attribution	The identification of who collected, recorded, or analyzed a piece of data, recorded as part of the data itself.
Chain of reliance	The sequence of parties who depend on a piece of data they did not produce and cannot independently verify, such as those relying on a certified test report.
Conformance	A determination that a measured value or result meets a specified requirement or limit.
Contemporaneous record	A record made at the time the work was performed rather than reconstructed afterward from memory.
Defensible record	A record complete enough that a competent person can reconstruct what was done, by whom, when, and under what conditions, and reach the same result from the same inputs.
Fabrication	Making up data or results and recording or reporting them as if genuine.
Falsification	Manipulating materials, equipment, or processes, or changing or omitting data, so that the record does not accurately reflect the work.
FFP triad	The three categories of research misconduct under United States federal policy: fabrication, falsification, and plagiarism.
Method shopping	Selecting an analysis, model, or acceptance test after seeing which one produces the preferred result.
Outlier	A data point that lies far enough from the others to warrant investigation; its exclusion is legitimate only under a basis defined before the results are seen.
Plagiarism	Appropriating another person's ideas, results, or words without appropriate credit.
Research misconduct	Fabrication, falsification, or plagiarism committed intentionally, knowingly, or recklessly; honest error and good-faith differences of judgment are excluded.
Responsible charge	The direct control and personal supervision of engineering work that a licensed engineer attests to when sealing a document.
Traceability	The property of a record that allows any value or change to be linked to its origin, author, time, and prior state.
Version control	A method of retaining the history of changes to a record so that every revision is traceable to its author and previous state.

© Dr Jeelan Moghraby, 2026

Appendix B: Disciplinary Case Studies

The following cases are drawn from the public disciplinary records of two state engineering boards: the Texas Board of Professional Engineers and Land Surveyors (TBPELS) and the Florida Board of Professional Engineers (FBPE). They were selected to cover different facets of data and reporting integrity: untruthful or fraudulent engineering assertions, misrepresentation of who performed sealed work, and negligent work that the sealed record presented as sound. State PE boards discipline more frequently for these conduct categories than for "data falsification" as a named offense, because large-scale data fraud, as in the Volkswagen and Kobe Steel matters, tends to be pursued through federal and criminal channels. Case references and outcomes are stated as published by each board.

Case 1: Fraudulent or deceitful written assertions (Texas)

***Reference and source**:* P.E. No. 63096, Katy, TX; TBPELS Case No. D-43032 (Board meeting November 20, 2025). Source: TBPELS disciplinary actions.

***Summary**:* The engineer failed to issue statements only in an objective and truthful manner and instead issued written assertions in the practice of engineering that were fraudulent or deceitful, and failed to practice engineering in a careful and diligent manner.

***Findings and outcome**:* The board found violations of 22 Tex. Admin. Code §§ 137.57(a) and 137.63(b)(6) and imposed a one-year active suspension, completion of an engineering ethics course, and a $3,000 administrative penalty.

***Course connection**:* This case maps directly to the duty to issue objective and truthful statements (Chapter 4; NSPE Fundamental Canon 3). The conduct sits in the reporting stage of the data lifecycle (Chapter 2). A defensible record and truthful reporting of what the work actually showed would have avoided the violation.

Case 2: Misrepresenting responsible charge through sealing (Texas)

***Reference and source**:* P.E. No. 131051, Houston, TX; TBPELS Case No. D-43205 (Board meeting November 20, 2025). Source: TBPELS disciplinary actions.

***Summary**:* The engineer sealed work that was not done by him or under his direct supervision, affixed or associated his seal in connection with work when his license status did not permit it, and failed to prevent the association of his professional identity with practices the board characterized as fraudulent or dishonest, including aiding the unlicensed practice of engineering.

***Findings and outcome**:* The board found violations of 22 Tex. Admin. Code §§ 137.33(b), 137.37(a)(2), 137.63(b)(3), and 137.63(c)(1), and imposed a two-year suspension (one year active, one year probated), completion of an engineering ethics course, and a $2,000 administrative penalty.

***Course connection**:* Sealing is the point where the data record and personal accountability meet (Chapter 2). Misrepresenting who performed work is a form of plagiarism and deceptive practice (Chapter 1, Table 1.1; NSPE Fundamental Canons 4 and 5). Confirming responsible charge before sealing is the controlling safeguard.

Case 3: Negligence in sealed engineering work (Florida)

***Reference and source**:* Florida Board of Professional Engineers, PE No. 38550; FBPE Case No. 2023062640. Source: FBPE disciplinary actions.

***Summary**:* The licensee was charged with negligence in the practice of engineering under Section 471.033(1)(g), Florida Statutes, and Rule 61G15-19.001(4), Florida Administrative Code. Licensee digitally signed and sealed engineering work that were materially deficient.

***Findings and outcome**:* The Board imposed costs of $3,671.60, completion of the Auburn University course "Basic Engineering Ethics and Professionalism," completion of the Board's Florida Laws and Rules Study Guide, and project reviews at six and 18 months for all fire alarm design projects signed and sealed by licensee.

***Course connection**:* Negligence differs from intentional misrepresentation (Chapter 1), but the sealed record presents negligent work as sound, so the public relies on it the same way. Independent review of the data and analysis behind a sealed document (Chapter 4) is the safeguard most likely to catch the deficiency before the seal is applied.