Transparency measurement

Dayana Spagnuelo[*], Cesare Bartolini[†], Gabriele Lenzini[†]

Interdisciplinary Centre for Security Reliability and Trust (SnT)

University of Luxembourg

{*firstname.lastname*}*@uni.lu*

This document intends to aid the understanding of a transparency measurement procedure. In Section 1 we present metrics descriptors in a format adapted from ISO/IEC 27004 standard[1]. The categories *Suitability*, *Computation* and *Considerations* were added to ease the understanding, and the categories *Frequency* and *Responsible parts* are not filled, as they depend heavily on the system being measured. Additionally, the category *Information need*, also suggested in the standard, was omitted. This category intends to clarify the contribution of each metric. We judged it unnecessary in our context, as the *Measure ID*, in combination with the requirement being measured already clarify that.

Section 2 exemplifies the evaluation process: we show, step by step, how to calculate the metrics to assess the quality of transparency on the Microsoft HealthVault[2], an online medical data service. Lacking any comparative analysis, this assessment exercise is not meant to suggest any judgement on the quality of transparency and on the legal compliance of that particular service, but rather it serves as an example of how to apply the metrics on a real system and of how to visualize of the result.

[*] Supported by FNR/AFR project 7842804 TYPAMED

[†] Supported by CORE/FNR project 11333956 DAPRECO

[1] ISO/IEC 27004 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation, 2^{nd} edition.

[2] `https://www.healthvault.com/lu/en`.

1 Measure descriptors

Measure ID	**Reachability**
Suitability	Applies to information and mechanisms;
Measure	Linear and inverse exponential
Computation	1. Determine a number k maximum number of interactions that is considered acceptable to perform in order to find the information/mechanism's output; 2. Whenever the system allows login, start analysing from the screen after the successful login; Otherwise start from the main screen; 3. Extensively search for information/mechanism that implement the requirement; 4. Stop when reaching the information or the expected output of the mechanism (even if incomplete); 5. Count the amount of interaction N_{int} needed to reach it from the initial screen; An interaction is a click, typing, or anything that requires the user to actively do something to change the current state of the system; 6. Measure $\mathcal{R}c$.
Formula/scoring	$\mathcal{R}c = \begin{cases} 1, & \text{if } 0 \leq N_{\text{int}} \leq k \\ e^{(1-\frac{N_{\text{int}}}{k})}, & \text{if } N_{\text{int}} > k \end{cases}$
Target	1
Implementation evidence	Any kind of information or mechanism's output; Number of acceptable interactions;
Frequency	
Responsible parties	
Data source	Documents; Notifications; Communications to users; Mechanism's output;
Reporting format	Grade; k; N_{int}
Considerations	In case the evidence is spread across multiple parts of the system, calculate the amount of interaction N_{int} needed to reach every single data source, and measure $\mathcal{R}c$ considering their sum.

Table 1: Reachability metric

Measure ID	**Portability**
Suitability	Applies to information and mechanisms;
Measure	Scale
Computation	1. Measure $\mathcal{P}$.
Formula/scoring	$\mathcal{P} = \begin{cases} 0, & \text{if no information available} \\ 0.2, & \text{if available in any open format} \\ 0.4, & \text{if available as a structured data} \\ 0.6, & \text{if available in a non-proprietary format} \\ 0.8, & \text{if uses URI} \\ 1, & \text{if based on linked data} \end{cases}$
Target	1
Implementation evidence	Any kind of information or mechanism's output;
Frequency	
Responsible parties	
Data source	Documents; Notifications; Communications to users; Mechanism's output;
Reporting format	Grade
Considerations	In case the evidence is spread across multiple parts of the system, calculate portability for every single data source, and consider the lowest grade.

Table 2: Portability metric

Measure ID	**Observability**
Suitability	Only suitable for information;
Measure	Proportion
Computation	1. Determine whether the information contains statements with claims or affirmations about the system's behaviour; only applicable if it does; 2. Select a total of $LS + NLS$ of statements, at least one per section/subject of the information; 3. Determine the number LS of statements which can be observed or linked to the system's process; 4. Determine the number NLS of statements which cannot be linked, either because not present, or dubious; 5. Measure $\mathcal{O}b$.
Formula/scoring	$\mathcal{O}b = \frac{LS}{LS+NLS}$
Target	1
Implementation evidence	Descriptive documents; List of entities;
Frequency	
Responsible parties	
Data source	Policies; Terms of use; Any document that describes the practice of the system;
Reporting format	Grade, statements
Considerations	In case the evidence is spread across multiple parts of the system consider everything as one single data source.

Table 3: Observability metric

Measure ID	**Accuracy**
Suitability	Only suitable for information;
Measure	Proportion
Computation	1. Determine the number LS of statements which can be observed or linked to the system's process; only applicable for those; 2. Determine the number ALS of statements that accurately (correctly and consistently with the user's experience) describe some part of the system's process; 3. Measure $\mathcal{A}c$.
Formula/scoring	$\mathcal{A}c = \frac{ALS}{LS}$
Target	1
Implementation evidence	Descriptive documents; List of entities;
Frequency	
Responsible parties	
Data source	Policies; Terms of use; Any document that describes the practice of the system;
Reporting format	Grade, statements
Considerations	Builds on top of Observability metric (see item 3); In case the evidence is spread across multiple parts of the system consider everything as one single data source.

Table 4: Accuracy metric

Measure ID	**Currentness**
Suitability	Applies to information and mechanisms;
Measure	Inverse exponential
Computation	1. Determine the maximum acceptable delay t_{max} in which the information or mechanism output should be made available; 2. Collect the time t taken for the system to provide the information or mechanism output in the same unit as the ideal time frame; 3. Measure $\mathcal{C}u$.
Formula/scoring	$\mathcal{C}u = \begin{cases} 1, & \text{if } t \leq t_{max} \\ 2^{-\left\lceil \frac{t - t_{max}}{t_{max}} \right\rceil}, & \text{if } t > t_{max} \end{cases}$
Target	1
Implementation evidence	Any kind of information or mechanism's output; The time in which the information was made available; The tolerable amount of time for the information to be made available;
Frequency	
Responsible parties	
Data source	Documents; Notifications; Communications to users; Mechanism's output;
Reporting format	Grade, t_{max}
Considerations	In case the evidence is spread across multiple parts of the system, calculate currentness for every single data source, and consider the lowest grade.

Table 5: Currentness metric

Measure ID	**Conciseness**
Suitability	Only suitable for information;
Measure	Average words per sentence
Computation	1. Determine the nature of the information, only applicable if it is a text (with at least one sentence); 2. Select a tool to aid calculating the average sentence length ASL; 3. Measure $\mathcal{C}o$.
Formula/scoring	$\mathcal{C}o = e^{-\frac{1}{50}(ASL-20)^2}$
Target	1
Implementation evidence	Any kind of information provided in text format
Frequency	
Responsible parties	
Data source	Documents; Notifications; Communications to the user;
Reporting format	Grade
Considerations	In case the evidence is spread across multiple parts of the system consider everything as one single data source.

Table 6: Conciseness metric

Measure ID	**Detailing**
Suitability	Only suitable for information;
Measure	Proportion
Computation	1. Separate the data source into n_I pieces of information (e.g., sections of a document, elements in a list, ...); 2. Determine a list of questions related to the requirement; [One question per subject in the requirement statement] OR [Apply the 5W (Who, What, Where, When and Why)]; 3. For each piece of information $i = 1 \dots n_I$ select a number P_i^D of pertinent questions for which details should be provided; non-pertinent questions should not be considered; 4. For each piece of information $i = 1 \dots n_I$ identify the number d_i of questions for which the details are provided, and number u_i of questions for which details are not provided, such that $d_i + u_i = P_i^D$ (do not consider how well explained the details are); 5. Measure $\mathcal{D}$.
Formula/scoring	$\mathcal{D} = \frac{\sum_{i=1}^{n_I} d_i}{\sum_{i=1}^{n_I} P_i^D}$
Target	1
Implementation evidence	Any kind of information or mechanism's output; The details it is supposed to provide to the user;
Frequency	
Responsible parties	
Data source	Documents; Notifications; Communications to users; Mechanism's output;
Reporting format	Grade, matrix representing the pieces of information i and the questions;
Considerations	In case the evidence is spread across multiple parts of the system consider everything as one single data source.

Table 7: Detailing metric

Measure ID	**Readability**
Suitability	Only suitable for information;
Measure	Flesch reading ease
Computation	1. Determine the nature of the information; Only applicable if it is a text (with at least one sentence); 2. Select a tool to aid calculating the average sentence length ASL and average number of syllables per word ASW; 3. Calculate $FRES$; 4. Measure $\mathcal{R}$.
Formula/scoring	$FRES = 206.835 - (1.015 \times ASL) - (84.6 \times ASW)$ $\mathcal{R} = \begin{cases} 0, & \text{if } FRES < 0 \\ \frac{FRES}{100}, & \text{if } 0 \leq FRES \leq 100 \\ 1, & \text{if } FRES > 100 \end{cases}$
Target	1
Implementation evidence	Any kind of information provided in text format.
Frequency	
Responsible parties	
Data source	Documents; Notifications; Communications to the user;
Reporting format	Grade
Considerations	In case the evidence is spread across multiple parts of the system consider everything as one single data source.

Table 8: Readability metric

Measure ID	**Effectiveness**
Suitability	Only suitable for mechanism;
Measure	Proportion
Computation	1. Separate the mechanism's output into n_I pieces of information (e.g., tool's output, if more than one tool is provided for the same requirement, elements in a list, $\ldots$); 2. Determine a list of questions a user intends to have answered when using the mechanism (i.e., the goals of the mechanism); [One question per subject in the requirement statement] OR [Apply the 5W (Who, What, Where, When and Why)]; 3. For each piece of information $i = 1 \ldots n_I$ select a number P_i^E of pertinent questions which should be answered by it; non-pertinent questions should not be considered; 4. For each piece of information $i = 1 \ldots n_I$ identify the number e_i of questions which are answered by the mechanism (goals reached), and number v_i of questions which are not answered (goals not reached), such that $e_i + v_i = P_i^E$; 5. Measure $\mathcal{E}$.
Formula/scoring	$\mathcal{E} = \frac{\sum_{i=1}^{n_I} e_i}{\sum_{i=1}^{n_I} P_i^E}$
Target	1
Implementation evidence	Mechanism's output;
Frequency	
Responsible parties	
Data source	Mechanism's output; The goals the mechanism is supposed to reach;
Reporting format	Grade, matrix representing the delivered outputs and the desired goals (questions);
Considerations	In case the evidence is spread across multiple parts of the system consider everything as one single data source.

Table 9: Effectiveness metric

Measure ID	**Operativeness**
Suitability	Only suitable for mechanism;
Measure	Proportion
Computation	1. Define the set of equivalence classes $E = C \cup R \cup U \cup D$, the union of all possible actions relevant to the system (e.g., create document, edit personal information, ...); where C contains create actions, R contains read actions, U contains update actions, D contains delete actions; 2. Select a sub-set of actions $A = \{a_0, a_1, \ldots, a_{k-1}\} : (A \subseteq E)$, that contains at least one action of each class (i.e., $(A \cap C \neq \emptyset) \wedge (A \cap R \neq \emptyset) \wedge (A \cap U \neq \emptyset) \wedge (A \cap D \neq \emptyset))$ 3. Measure $\mathcal{O}_A$.
Formula/scoring	$\mathcal{O}_A = \lfloor n/k \rfloor$
Target	1
Implementation evidence	Mechanism's output
Frequency	
Responsible parties	
Data source	Mechanism's output, Actions to be tested;
Reporting format	Grade; set of actions A tested
Considerations	In case the evidence is spread across multiple parts of the system consider everything as one single data source.

Table 10: Operativeness metric

2 Evaluation of Microsoft HealthVault

2.1 Information-Based Requirements

2.1.1 111.1 – The system must provide the user with real time information on physical data storage and data storage location of different types of data

The information used to measure this requirement can be found in the "Microsoft Privacy Statement", under "Other Important Privacy Information" – "Where We Store and Process Personal Data" (WPD).

Metric	Attributes	Grade
Reachability	$k = 3$; $N_{\text{int}} = 3$	1
Portability		0.8
Observability	Statements: 1. "Typically, the primary storage location is in the customer's region or in the United States, often with a backup to a data centre in another region." 2. "The storage location(s) are chosen in order to operate efficiently, to improve performance and to create redundancies in order to protect the data in the event of an outage or other problem." 3. "When we engage in such transfers, we use a variety of legal mechanisms, including contracts, to help ensure your rights and protections travel with your data." 4. "Microsoft Corporation complies with the EU-US Privacy Shield Framework and Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal information transferred from the European Union and Switzerland to the United States." 5. "If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern."	0
Accuracy		N/A
Currentness		N/A
Conciseness		0.9626282259
Detailing	See Table 12	0.25
Readability		0.227023

Table 11: Attributes and grades per metric referring to requirement 111.1.

	Delivered Details
Desired Details	WPD
Is the information provided in real time?	
Is there information on physical storage?	
Where is the data stored?	✓
Which type of data is stored?	

Table 12: Detailing matrix 111.1: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

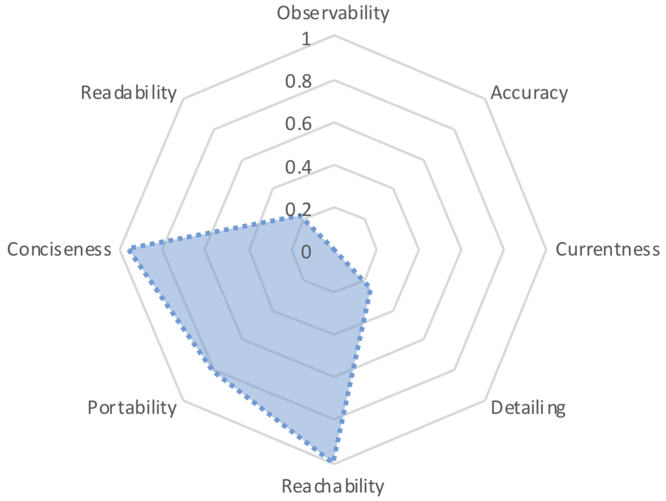


Figure 1: Transparency measurement of requirement 111.1.

2.1.2 111.2 – The system must inform the user on how data are stored and who has access to them.

The information used to measure this requirement can be found in the "Microsoft Privacy Statement", under "Other Important Privacy Information" – "Security of Personal Data" (SPD).

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 3$	1
Portability		0.8
Observability	Statements: 1. "We store the personal data you provide on computer systems that have limited access and are in controlled facilities." 2. "When we transmit highly confidential data (such as a credit card number or password) over the Internet, we protect it through the use of encryption." 3. "Microsoft complies with applicable data protection laws, including applicable security breach notification laws."	0
Accuracy		N/A
Currentness		N/A
Conciseness		0.9372548956
Detailing	See Table 14	0.5
Readability		0.2593

Table 13: Attributes and grades per metric referring to requirement 111.2.

	Delivered Details
Desired Details	SPD
How is data stored?	✓
Who has access to data?	

Table 14: Detailing matrix 111.2: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

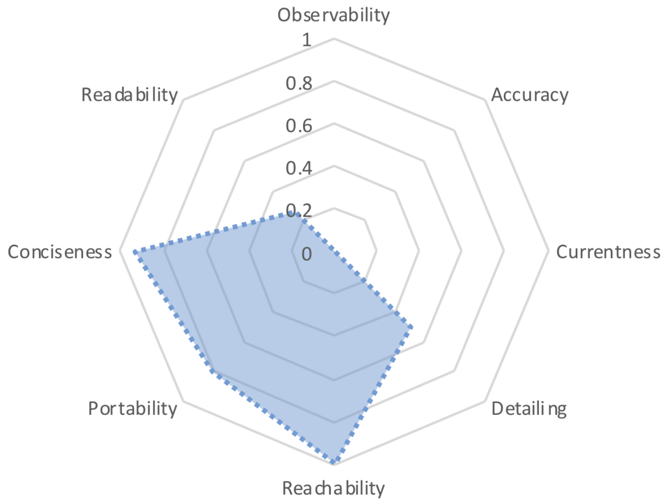


Figure 2: Transparency measurement of requirement 111.2.

2.1.3 111.5 – The system must inform the user how it is assured that data are not accessed without authorisation.

The information used to measure this requirement can be found in the "Microsoft Privacy Statement", under "Other Important Privacy Information" – "Security of Personal Data." (SPD).

Metric	Attributes	Grade
Reachability	$k = 3$; $N_{\text{int}} = 3$	1
Portability		0.8
Observability	Statements: 1. "We store the personal data you provide on computer systems that have limited access and are in controlled facilities." 2. "When we transmit highly confidential data (such as a credit card number or password) over the Internet, we protect it through the use of encryption." 3. "Microsoft complies with applicable data protection laws, including applicable security breach notification laws."	0
Accuracy		N/A
Currentness		N/A
Conciseness		0.9372548956
Detailing	See Table 16	1
Readability		0.2593

Table 15: Attributes and grades per metric referring to requirement 111.5.

	Delivered Details
Desired Details	SPD
How is it assured that data are not accessed without authorisation?	✓

Table 16: Detailing matrix 111.5: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

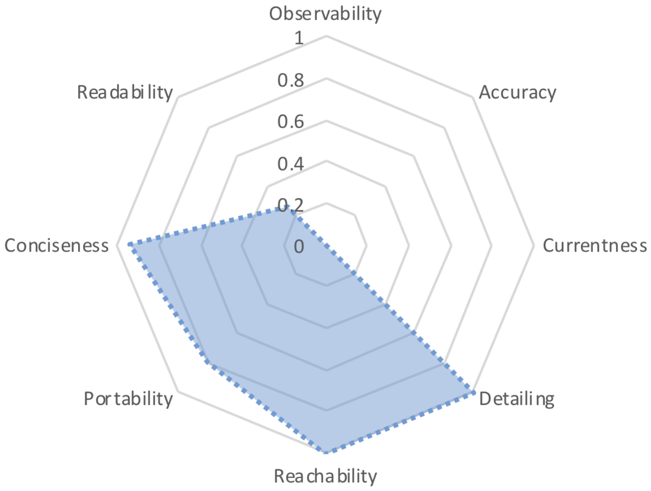


Figure 3: Transparency measurement of requirement 111.5.

2.1.4 111.6 – The system should make available a document that describes the adopted mechanisms for securing data against data loss as well as data privacy vulnerabilities.

The information used to measure this requirement can be found in the “Help”, under “Privacy and Security” – “How does HealthVault help keep my information private?” (KIP).

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 3$	1
Portability		0.8

Observability	Statements: 1. “We apply security and privacy standards throughout the HealthVault development process.” 2. “Microsoft won’t use your information in HealthVault to personalise ads or services without explicit permission.” 3. “Microsoft HealthVault allows you to manage access not just by other people, but by apps you use as well. ” 4. “HealthVault servers are located in controlled facilities.” 5. “All health information transmitted between HealthVault servers and program providers’ systems is encrypted.” 6. “When we back up data, the media are encrypted.”	0.17
Accuracy	Statement 3.	1
Currentness		N/A
Conciseness		0.5388748092
Detailing	See Table 18	0.5
Readability		0.356684

Table 17: Attributes and grades per metric referring to requirement 111.6.

	Delivered Details
Desired Details	KIP
Which are the mechanisms adopted for securing data against data loss?	
Which are the mechanisms adopted for securing data against privacy vulnerability?	✓

Table 18: Detailing matrix 111.6: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

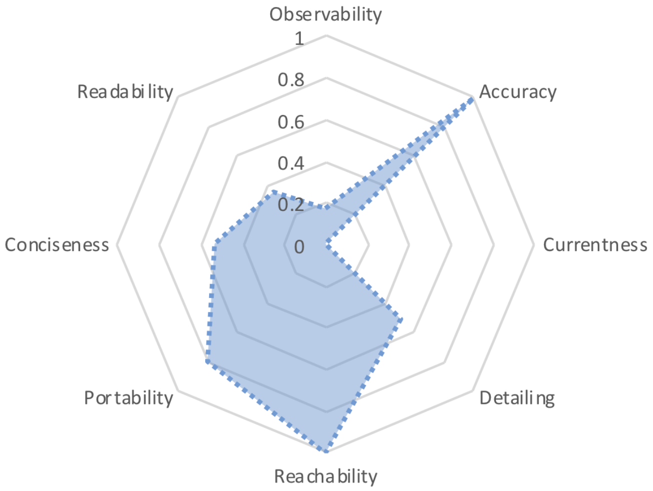


Figure 4: Transparency measurement of requirement 111.6.

2.1.5 111.7 – The system should make available a document that describes the procedures and mechanisms planned in cases of security breaches on the user's data.

The information used to measure this requirement can be found in the "Help", under "Privacy and Security" – "What happens if someone gains access to my HealthVault account?" (GAA)

Metric	Attributes	Grade
Reachability	$k = 3$; $N_{\text{int}} = 3$	0.8
Portability		0.8
Observability	Statements: 1. "If we learn of any potential breach of a HealthVault account, we will investigate, and, where appropriate, take actions possibly including blocking or suspending access to your account." 2. "If we determine there might have been a breach of your account, we will notify you via the contact information you have provided in your account." 3. "To provide an alternative contact address: Sign in to HealthVault. In the upper right, click your name and then click Account settings. Under Security, click Change security info. Enter the alternative contact information and click Save."	0.33
Accuracy	Statement 3.	1
Currentness		N/A
Conciseness		0.8241176336

Detailing	See Table 20	1
Readability		0.4248765

Table 19: Attributes and grades per metric referring to requirement 111.7.

	Delivered Details
Desired Details	GAA
Which are the procedures planned in case of security breach?	✓
Which are the mechanisms planned in case of security breach?	✓

Table 20: Detailing matrix 111.7: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

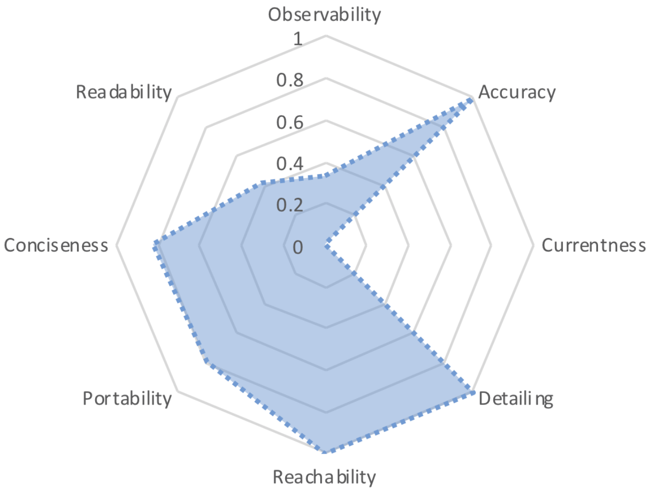


Figure 5: Transparency measurement of requirement 111.7.

2.1.6 111.9 – the user must be made aware of the consequences of their possible choices in an unbiased manner.

The information used to measure this requirement can be found in the "Sharing" section, as a warning before inviting someone to share the personal data. Additionally, further information can be found in the following page, under "What can a record custodian do?" (WCD).

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 2 + 1$	1

Portability		0.6
Observability	Statements: 1. “Sharing your record with a person you trust allows them to see, update, or delete information, depending on the level of access you give them.” 2. “A custodian is someone who has full access to all the information in a HealthVault record, with the ability to see, change, add to, share and delete any of that information.” 3. “Custodians can see information marked as confidential by other users, and they can see a history of all changes made to the record, including deleted items in the HealthVault trash.” 4. “Custodians can permanently delete information from the record.” 5. “In US accounts, custodians can manage Direct email addresses and send Direct messages on behalf of the record.” 6. “All custodians have equal access to the record.” 7. “Be very selective about who you give custodian access to, since they will have full control over the record, including the ability to remove your access to it.”	0.86
Accuracy	Statements 1 to 7.	1
Currentness	$t_{max} = 5s$ (before the actual choice, but at most 5 seconds after the user enters the sharing section)	1
Conciseness		0.9866420204
Detailing	See Table 22	1
Readability		0.401633

Table 21: Attributes and grades per metric referring to requirement 111.9.

	Delivered Details	
Desired Details	Sharing	WCD
What are the consequences?	✓	✓
Is the information unbiased?	✓	✓

Table 22: Detailing matrix 111.9: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

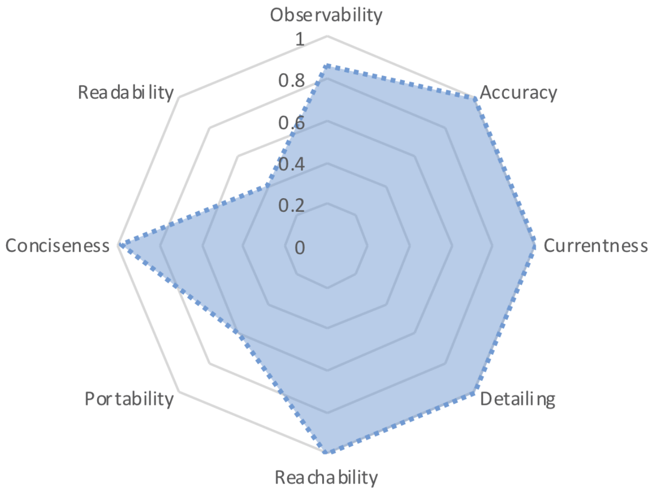


Figure 6: Transparency measurement of requirement 111.9.

2.1.7 111.11 – The system must inform the user about storage in other countries and compliance issues related to this storage with respect to laws and regulations of both the other country and their own country.

The information used to measure this requirement can be found in the "Microsoft Privacy Statement", under "Other Important Privacy Information" – "Where We Store and Process Personal Data." (WPD)

Metric	Attributes	Grade
Reachability	$k = 3$; $N_{\text{int}} = 3$	1
Portability		0.8

Observability	Statements: 1. “Typically, the primary storage location is in the customer’s region or in the United States, often with a backup to a data centre in another region.” 2. “The storage location(s) are chosen in order to operate efficiently, to improve performance and to create redundancies in order to protect the data in the event of an outage or other problem.” 3. “When we engage in such transfers, we use a variety of legal mechanisms, including contracts, to help ensure your rights and protections travel with your data.” 4. “Microsoft Corporation complies with the EU-US Privacy Shield Framework and Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal information transferred from the European Union and Switzerland to the United States.” 5. “If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern.”	0
Accuracy		N/A
Currentness		N/A
Conciseness		0.9626282259
Detailing	See Table 24	1
Readability		0.227023

Table 23: Attributes and grades per metric referring to requirement 111.11.

	Delivered Details
Desired Details	WPD
Are data stored in other countries?	✓
Are there compliance issues related to that?	✓

Table 24: Detailing matrix 111.11: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

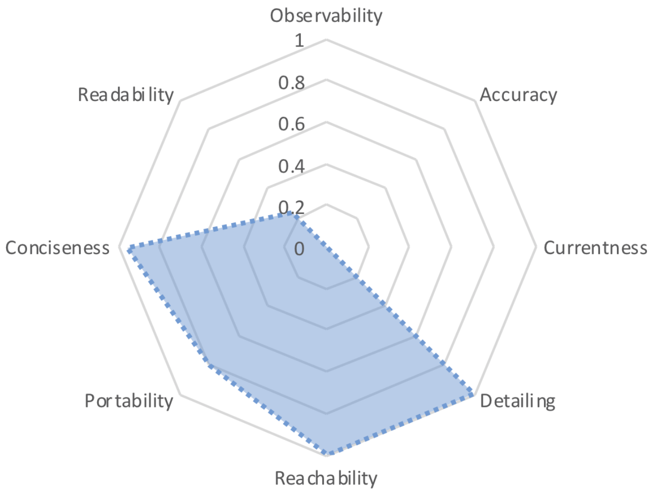


Figure 7: Transparency measurement of requirement 111.11.

2.1.8 111.13 – The system must inform the user on how to protect data or how data are protected.

The information used to measure this requirement can be found in the “Help”, under “Privacy and Security” – “How does HealthVault help keep my information private?” (KIP).

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 3$	1
Portability		0.8
Observability	Statements: 1. “We apply security and privacy standards throughout the HealthVault development process.” 2. “Microsoft won’t use your information in HealthVault to personalise ads or services without explicit permission.” 3. “Microsoft HealthVault allows you to manage access not just by other people, but by apps you use as well.” 4. “HealthVault servers are located in controlled facilities.” 5. “All health information transmitted between HealthVault servers and program providers’ systems is encrypted.” 6. “When we back up data, the media are encrypted.”	1
Accuracy	Statement 3.	1
Currentness		N/A
Conciseness		0.53887480925
Detailing	See Table 26	0.5

Readability		0.356684

Table 25: Attributes and grades per metric referring to requirement 111.13.

	Delivered Details
Desired Details	KIP
How can someone protect data?	
How is data protected?	✓

Table 26: Detailing matrix 111.13: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

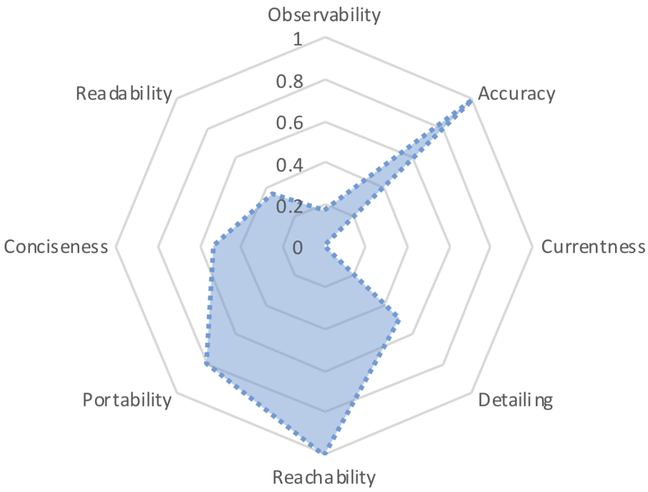


Figure 8: Transparency measurement of requirement 111.13.

2.1.9 111.17 – The system must make available a document explaining the procedures for leaving the service and taking the data out from the service.

The information used to measure this requirement can be found in the “Help”, under “Your HealthVault Account” – “How do I close my HealthVault account?” (CMA). Additionally, further information can be found in “How do I export and save health information from HealthVault?” (ESI).

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 3 + 1$	0.7165313106
Portability		0.8

Observability	Statements: 1. “Once your account has been closed, any information that you had stored in your account will be permanently deleted, although data may remain on our servers for 90 days.” 2. “To delete your account: Sign in to HealthVault. In the upper right, click your name and then click Account settings. At the bottom of the page, click Close account. Carefully review the information on the page, then click Close my account.” 3. “The exception is if there are other custodians of records in your account. In that case, youll be notified at the time you close the account, and those records will not be deleted.” 4. “You can export and save your health information in two ways: as a spreadsheet;” 5. “or as a CCR or CCD or HTML file.” 6. “To save health information as a spreadsheet: Sign in to HealthVault. On the left side of the page, click the name of the type of information you want to save as a spreadsheet. You’ll see the list view for that type of data. Click Export. In the browser message that appears, click Save. Your information will be saved in a spreadsheet format (.csv) that can be opened in Excel or other spreadsheet software.” 7. “You can create a CCR or CCD with information from your HealthVault record, but keep in mind that CCRs and CCDs dont support all types of health information, so they won’t necessarily contain everything in your record.” 8. “To save information in your HealthVault record as a CCR or CCD or HTML file: Sign in to HealthVault. On the Home page, click Current and then click Export. Select the file format that you want to use. Select the type or types of information that you want to export. If you want to, select the date range for the data. Click Export. In the browser message that appears, click Save. Your information will be saved as a file on your computer.”	0.88
Accuracy	Statements: 2 to 8. Statement 3 is not considered accurate.	0.86
Currentness		N/A

Conciseness		0.5956142816
Detailing	See Table 28	1
Readability		0.6395535

Table 27: Attributes and grades per metric referring to requirement 111.17.

	Delivered Details	
Desired Details	CMA	ESI
How to proceed to leave the service?	✓	
How to proceed to take data out from the service?		✓

Table 28: Detailing matrix 111.17: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

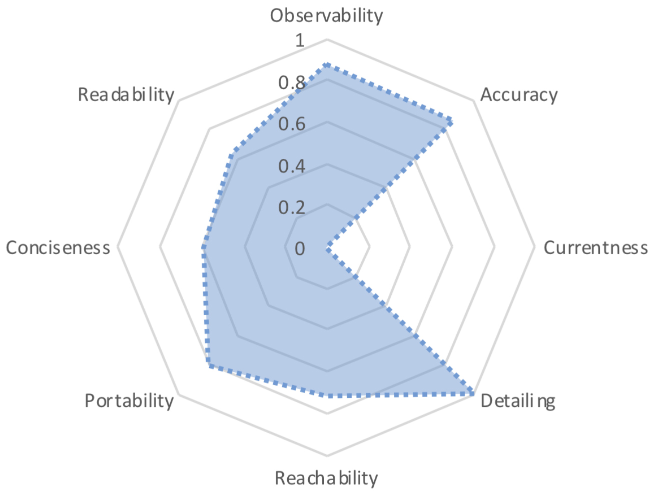


Figure 9: Transparency measurement of requirement 111.17.

2.1.10 111.19 – The system must provide the user with disclosure of policies, regulations or terms regarding data sharing, processing and the use of data.

The information used to measure this requirement can be found in the "Microsoft Privacy Statement", and it is spread throughout several sections: "Personal Data That We Collect" (PDC), "How We Use Personal Data" (UPD), "Reasons We Share Personal Data" (SPD), "Cookies & Similar Technologies" (CST), "Other Important Privacy Information" (IPI), and "Microsoft Health Services" (MHS). To test for Observability and Accuracy we only consider statements exclusively related to HealthVault (MHS).

Metric	Attributes	Grade
Reachability	$k = 3$; $N_{\text{int}} = 1 + 1$	1
Portability		0.8

Observability	Statements: 1. “You can use more than one credential with HealthVault to help ensure continued access”; 2. “You can add or remove data to a health record you manage at any time”; 3. “As a custodian, you can share data in a health record with another person by sending an email invitation through HealthVault. You can specify what type of access they have (including custodian access), how long they have access, and whether they can modify the data in the record”; 4. “In the United States, we enable participating providers to obtain reports about whether the information they send to a record is used”; 5. “You can review, edit or delete your HealthVault account data, or close your HealthVault account at any time”; and 6. “You can unsubscribe from these emails [communications] at any time”.	0.83
Accuracy	Statements 1, 2, 3, 5 and 6. Statement 1 is not considered accurate.	0.8
Currentness		N/A
Conciseness		0.9620950775
Detailing	See Table 30	1
Readability		0.3481985

Table 29: Attributes and grades per metric referring to requirement 111.19.

	Delivered Details					
Desired Details	DWC	UPD	SPD	CST	IPI	MHS
How is data shared? With whom? For what purpose?			✓			
How is data processed? For what purpose?	✓	✓				
How is data used? For what purpose?				✓	✓	✓

Table 30: Detailing matrix 111.19: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

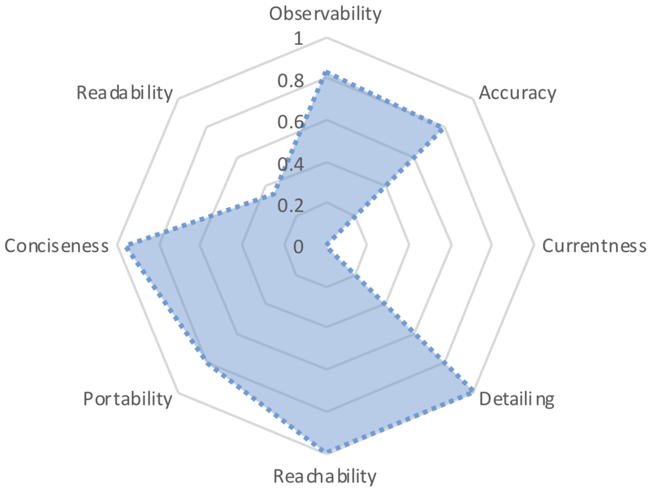


Figure 10: Transparency measurement of requirement 111.19.

2.1.11 211.5 – The system must inform the user if and when data is gathered, inferred or aggregated.

The information used to measure this requirement can be found in the "Microsoft Privacy Statement" (MPS), and it is spread throughout the entire document. To test for Observability and Accuracy we only consider statements related to collection of personal data ("Personal Data That We Collect").

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 1$	1
Portability		0.8
Observability	Statements: 1. "The data we collect depends on the context of your interactions with Microsoft and the choices that you make, including your privacy settings and the products and features that you use. We also obtain data about you from third parties." 2. "Where providing the data is optional, and you choose not to share personal data, features like personalisation that use such data will not work for you."	0
Accuracy		N/A
Currentness		N/A
Conciseness		0.8671199163
Detailing	See Table 32	0.5
Readability		0.4592695

Table 31: Attributes and grades per metric referring to requirement 211.5.

	Delivered Details
Desired Details	MPS
Is information gathered?	✓
Is information inferred?	✓
Is information aggregated?	✓
When is information gathered?	
When is information inferred?	
When is information aggregated?	

Table 32: Detailing matrix 211.5: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

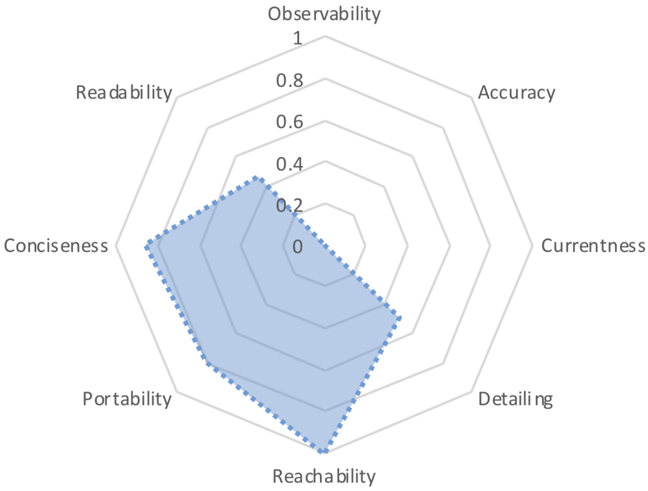


Figure 11: Transparency measurement of requirement 211.5.

2.1.12 221.5 – The system must provide the user with evidence regarding permissions history for auditing purposes.

The information used to measure this requirement can be found in the "Record history" section, under "Miscellaneous and access-related changes to Username's record" (MAC).

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 2$	1
Portability		0.6
Observability		N/A
Accuracy		N/A
Currentness	$t_{max} = 10s$	1
Conciseness		N/A
Detailing	See Table 34	1

Readability		N/A

Table 33: Attributes and grades per metric referring to requirement 221.5.

	Delivered Details
Desired Details	MAC
Is there information regarding permission history?	✓

Table 34: Detailing matrix 221.5: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

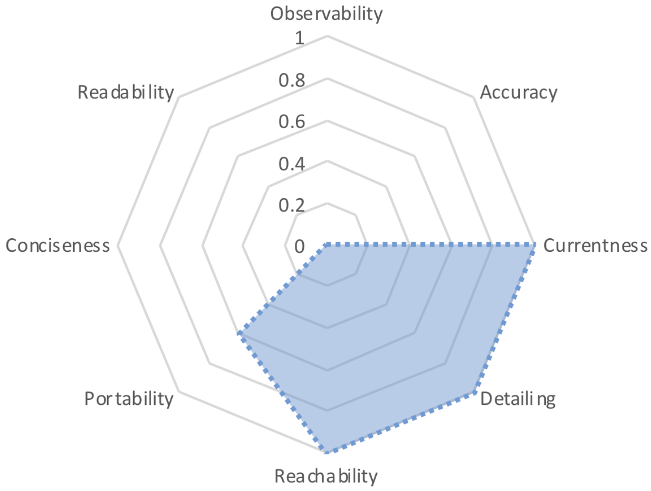


Figure 12: Transparency measurement of requirement 221.5.

2.2 Mechanism-Based Requirements

2.2.1 112.1 – The system must provide the user with mechanisms for accessing personal data.

The evidence used to measure this requirement can be found in the "Home" page.

Metric	Attributes	Grade
Reachability	$k = 3$; $N_{\text{int}} = 0$	1
Portability		0.6
Currentness	$t_{max} = 10s$	1
Effectiveness	See Table 36	1
Operativeness	A = {createData, updateData, deleteData, createSharedData, updateSharedData, deleteSharedData}	1

Table 35: Attributes and grades per metric referring to requirement 112.1.

	Delivered Outputs
Desired Goals	Home
Does the mechanism provide access to personal data?	✓

Table 36: Effectiveness matrix 112.1: desirable goals compared with the real outputs. Greyed-out cells represent the non-pertinent goals.

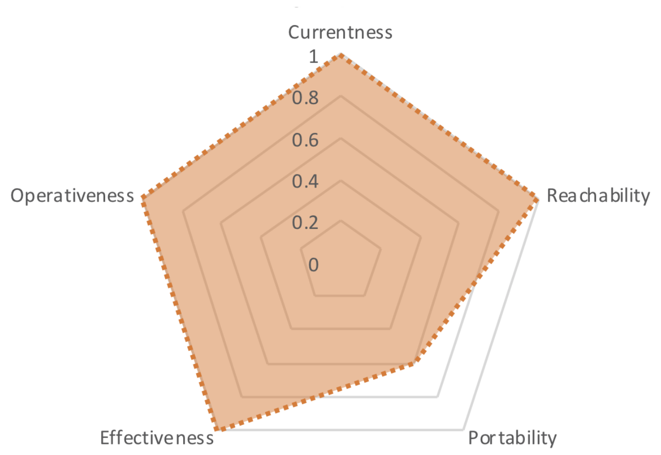


Figure 13: Transparency measurement of requirement 112.1.

2.2.2 222.1 – The system must provide the user with audit mechanisms.

The evidence used to measure this requirement can be found in the "Record history" section, under "All changes in the last 6 months" (CLM), and also "Views of Username's record in the last 30 days" (VUR).

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 2 + 2$	0.7165313106
Portability		0.6
Currentness	$t_{max} = 10s$	1
Effectiveness	See Table 38	0.7
Operativeness	$A = \{$createData, readData, updateData, deleteData$\}$	1

Table 37: Attributes and grades per metric referring to requirement 222.1.

	Delivered Outputs	
Desired Goals	CLM	VUR
What is the action?	✓	✓
When did it happen?	✓	✓
What was the outcome?		
From what source/application?	✓	✓
Which data suffered the action?	✓	

Table 38: Effectiveness matrix 222.1: desirable goals compared with the real outputs. Greyed-out cells represent the non-pertinent goals.

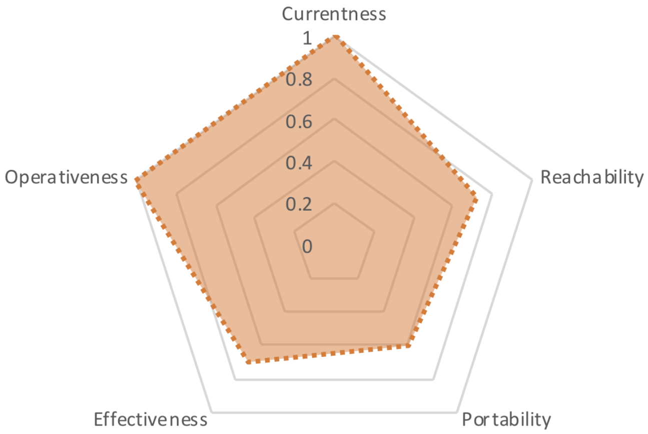


Figure 14: Transparency measurement of requirement 222.1.

2.2.3 232.1 – The system must provide the user with accountability mechanisms.

The evidence used to measure this requirement can be found in the “Record history” section, under “All changes in the last 6 months” (CLM), and also “Views of Username’s record in the last 30 days” (VUR).

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 2 + 2$	0.7165313106
Portability		0.6
Currentness	$t_{max} = 10s$	1
Effectiveness	See Table 40	0.75
Operativeness	$A = \{$createData, readData, updateData, deleteData$\}$	1

Table 39: Attributes and grades per metric referring to requirement 232.1.

	Delivered Outputs	
Desired Goals	CLM	VUR
What is the action?	✓	✓
When did it happen?	✓	✓
What was the outcome?		
Who did the action?	✓	✓
From what source/application?	✓	✓
Which data suffered the action?	✓	

Table 40: Effectiveness matrix 232.1: desirable goals compared with the real outputs. Greyed-out cells represent the non-pertinent goals.

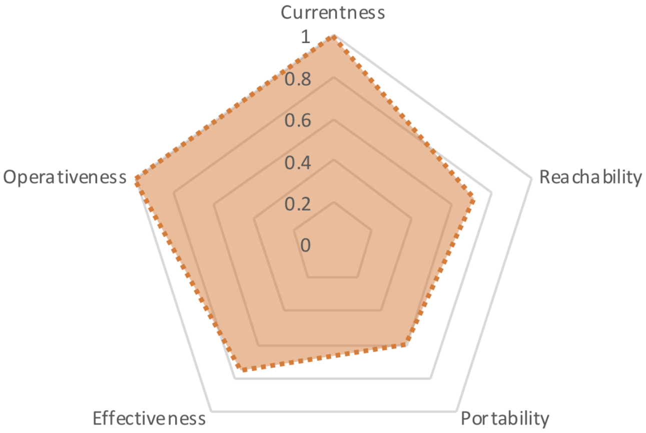
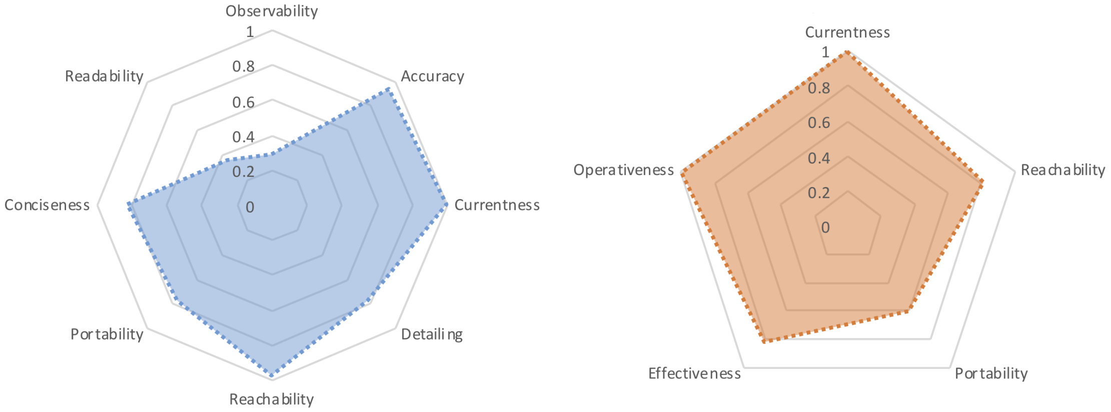


Figure 15: Transparency measurement of requirement 232.1.

2.2.4 Summary

In what follows, two radar charts are presented to summarise the grades achieved by Microsoft HealthVault in the transparency measurement. The chart depicted in Figure 16a represents the average grade achieved by the Information-based requirements analysed. While the one in Figure 16b represents the average grade achieved by Mechanisms-based ones. Metrics not applied (grade shown as N/A) are not counted in the average. As the requirements are evaluated with regard to every transparency quality, this evaluation reaches Transparency Evaluation Assurance Levels (TEAL)4.



(a) Average of grades for Information-based requirements.

(b) Average of grades for Mechanism-based requirements.

Figure 16: Average results of the transparency measurement in Microsoft HealthVault.